



**School Board Special Meeting  
Monday, June 13, 2022; 5:00 PM  
ECC Room 350**

**I. Determination of Quorum and Call to Order**

**II. Discussion**

**A. Strategic Plan Monitoring Report**

**Description:** District staff, students, and community members met for two days in April to receive reports, monitor, assess and provide feedback on District progress towards meeting our Strategic Plan outcomes and benchmarks.

**Presenter(s):** Denise Pontrelli and Paula O'Loughlin, SiteLogiQ

**B. Panorama Student and Staff Data Presentation**

**Description:** The Panorama Well-being and Engagement surveys were administered to Edina Public School staff and students in grades 3-12 in March 2022. Specific quantitative responses are included in the packet and qualitative summary responses to the open-ended questions are included in the slide presentation.

**Presenter(s):** Dr. Randy Smasal, Assistant Superintendent

**C. Edina Virtual Pathway Update**

**Description:** Update and discussion on current Edina Virtual Pathway progress.

**Presenter(s):** Steven Cullison, Edina Virtual Pathway Coordinator; Natasha Monsaas-Daly, Director of Media and Technology Services; Jody De St. Hubert, Director of Teaching and Learning; and Michael Walker, Digital Learning Specialist

**D. 2021-2022 Technology Plan**

**Description:** Strategy C.6 of EPS Strategic Plan tasks the district with completing a comprehensive review of technology used by staff and students. An outcome of this objective would be for the district to adopt an updated technology plan. Year one of development of this plan was focused on an audit of our current systems, processes, and needs. This report reflects the findings of this audit, as well as next steps.

**Presenter(s):** Natasha Monsaas-Daly, Director of District Media and Technology

**III. Action**

**A. Board Officer Approval**

**Description:** Due to moving out of the state, Vice Chair Leny Wallen-Friedman is no longer on the board as of May 31. This has left the position of Vice Chair vacant and needs to be filled. In filling the position of Vice Chair, other board roles could need to be filled as well.

**Presenter(s):** Board Chair Erica Allenburg

**Recommendation:** Chair Allenburg will have a recommendation for the board to fill the positions at the meeting.

**B. Endpoint Detection and Response RFP Proposal Acceptance - Carbon Black**

**Description:** EDR is a cybersecurity measure that provides monitoring and collection of endpoint data that may indicate a threat or threat patterns. This is a crucial piece of our cybersecurity posture. As threats increase, Edina Public Schools will need to continue to



update and maintain our security stance. We are committed to ensuring that staff and student data and systems are safe and secure.

**Presenter(s):** Natasha Monsaas-Daly, Director, District Media & Technology Services

**Recommendation:** Approve recommendation

**IV. Board Chair Updates**

**V. Superintendent Updates**

**VI. Closed Session (7:00-8:00 PM)**

**A. Legal Issue**

- *Closed Session pursuant to Minnesota Statutes Section 13D.05, subdivision 3(b), to engage in discussions with the School Board's legal counsel related to litigation that has been filed against the District in the case of Otto v. ISD 273, Court File No. 22-cv-00005-KMM-BRT. The Board seeks legal advice on the status of the matter, alleged claims against the District, the District Attorney's analysis of the same, the District's options for current matters to address, strategic considerations and the potential settlement or other resolution of the matter.*

**VII. Adjournment**





**Board Meeting Date:** 6/13/2022

**TITLE:** Strategic Plan Monitoring Report

**TYPE:** Discussion

**PRESENTER(S):** Denise Pontrelli and Paula O'Loughlin, SitelogiQ

**BACKGROUND:** District staff, students, and community members met for two days in April to receive reports, monitor, assess and provide feedback on District progress towards meeting our Strategic Plan outcomes and benchmarks.

**DESIRED OUTCOMES FROM THE BOARD:** Review presentation

**ATTACHMENTS:** Edina Strategic Plan Core Planning Team Process Presentation



# Edina Strategic Plan Core Planning Team Process

June 13, 2022





# Agenda

- Introductions
- Purpose
- Overview of Process
- Q & A





# School IQ Partners



**Denise Pontrelli**  
Learning, Innovation and  
Design Director



**Paula O'Loughlin**  
Education  
Consultant



**Matt Helgerson**  
Senior Education  
Consultant



# Purpose

To *support the monitoring process*, a Core Planning Team will be established to *receive yearly updates on our progress* in the implementation of the Strategic Plan. The team will *analyze the information provided to determine the extent to which we are on track to meet our timelines and with the intent of the plan.*

This stakeholder feedback is important as we continue to implement the plan. Feedback will be *summarized and shared with the school board, which might include recommendations for modifications or additional steps* to ensure the plan is realized by the 2027 timeline.



# Edina Public Schools Core Beliefs and Strategies

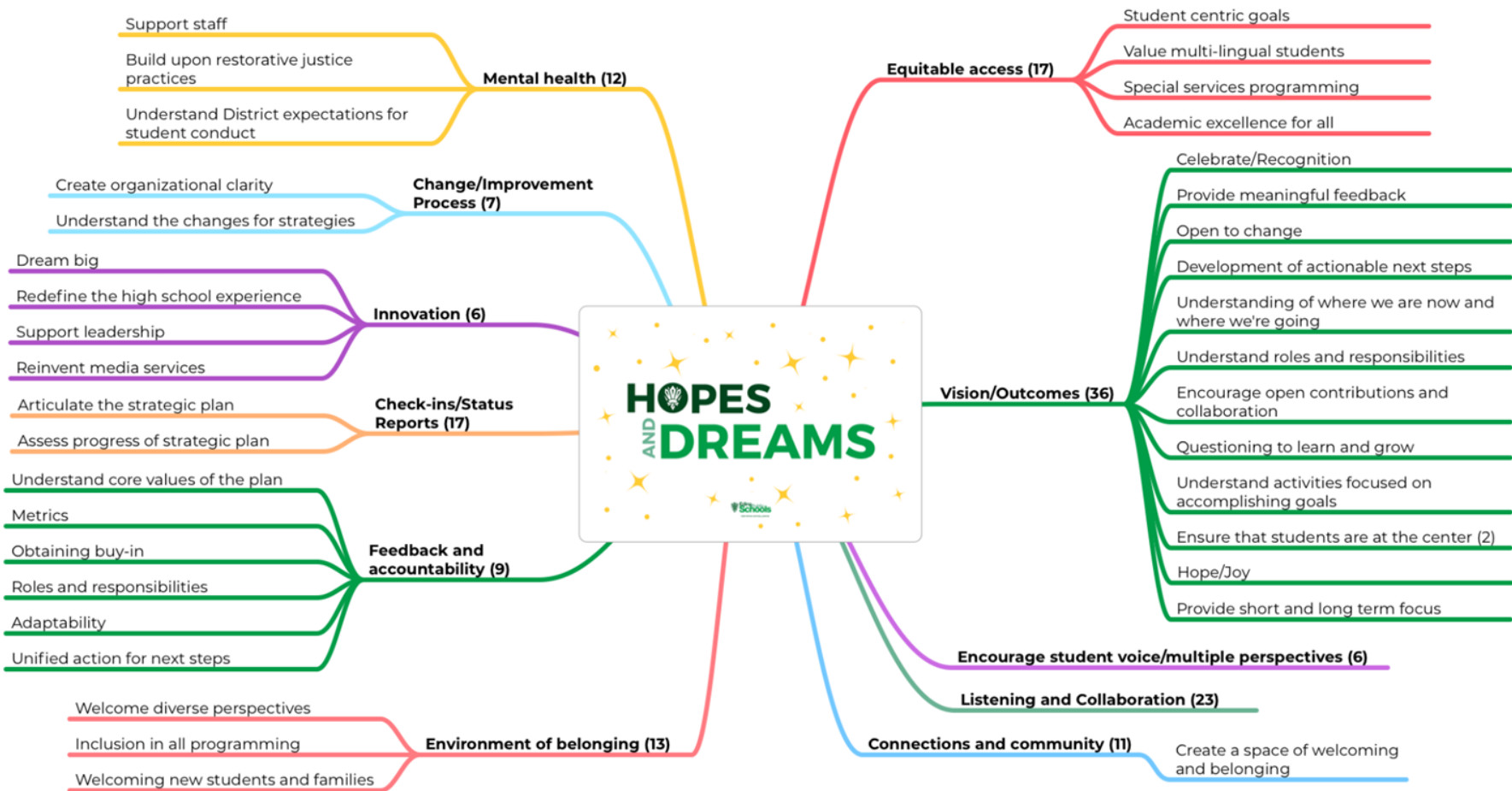




# Overview of Process

- Welcome and Grounding activity – Dr. Stanley, Superintendent
- Hopes and Dreams Activity
- Overview of the monitoring and evaluation process for EPS
- Progress Reports on Strategy Areas: Advance Academic Excellence, Growth and Readiness, Ensure and Equitable and Inclusive Culture, Foster Positive Learning Environments and Whole Student Support-Develop Leadership Throughout the District, Engage Parents, Schools and Community
- SOAR Process and Analysis: Strengths, Opportunities, Aspirations & Results (with Key Concepts and Themes for leadership to examine)
- Key Messages for the Community







# Priority Strategy – Progress Reports





# SOAR Analysis

## STRENGTHS

**What EPS does well; strengths also include key assets, resources, and accomplishments**

- What are we most proud of?
- What makes us unique?
- What do we provide that is world class?
- What strengths are most valuable in our marketplace?

## OPPORTUNITIES

**Circumstances that EPS can leverage so each and every student can discover their possibilities and thrive**

- What partnerships would benefit even more of our students?
- What threats do we see that can be reframed as opportunities?
- What needs and wants are we currently not fulfilling for our internal and external stakeholders?

## ASPIRATIONS

**An expression of what we want EPS to be and achieve in the future**

- What do we want to achieve in the future?
- What are we passionate about?
- What strategies and actions will support our best future school district?
- How can we continue to make a difference?

## RESULTS

**Tangible outcomes and measures that demonstrate we've achieved our goals and aspirations**

- What measures will tell us we are on track to achieve at our highest levels?
- How do we translate our vision into tangible outcomes?
- How do we know when we've achieved our goals?





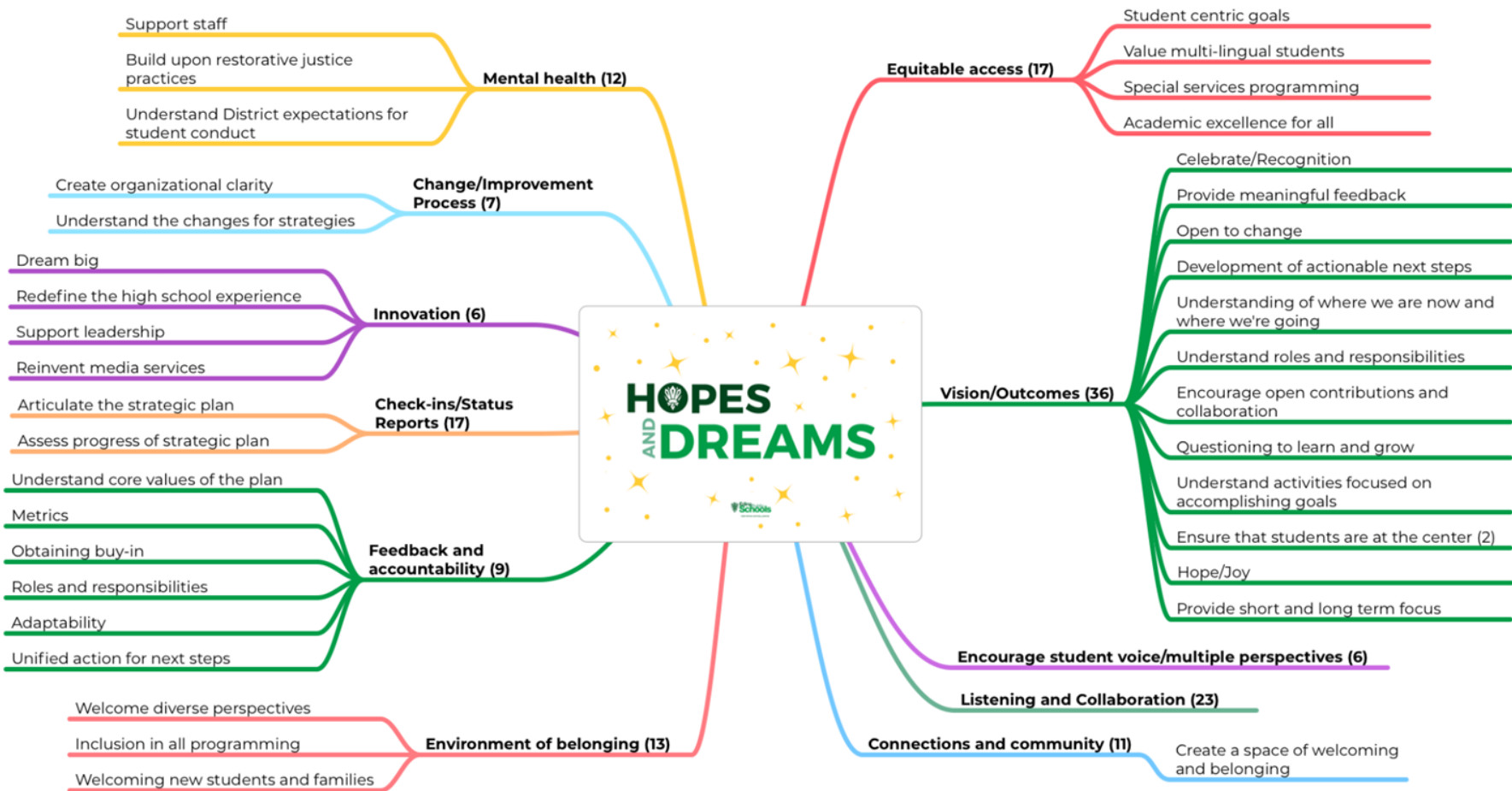




# Mind Map Analysis

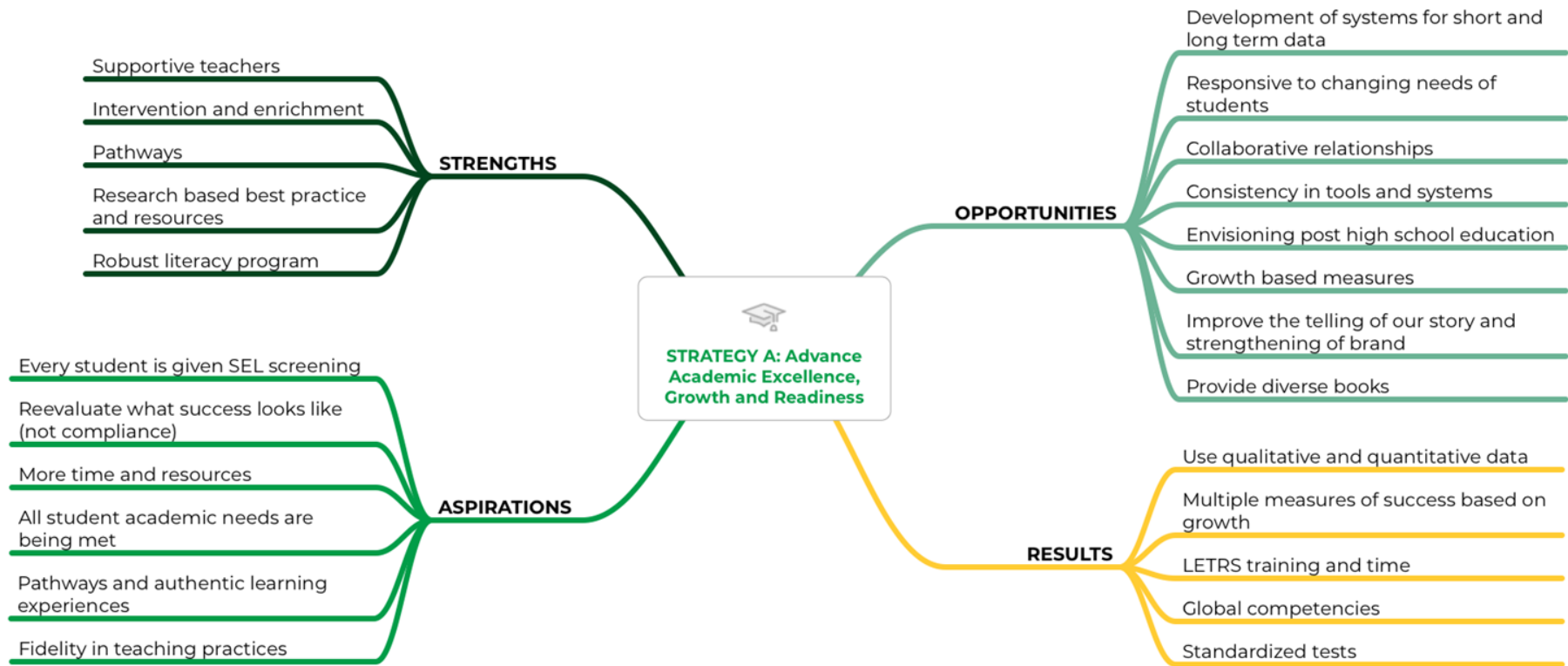
- What celebrations do we highlight?
- What might we modify?
- What might we recommend?





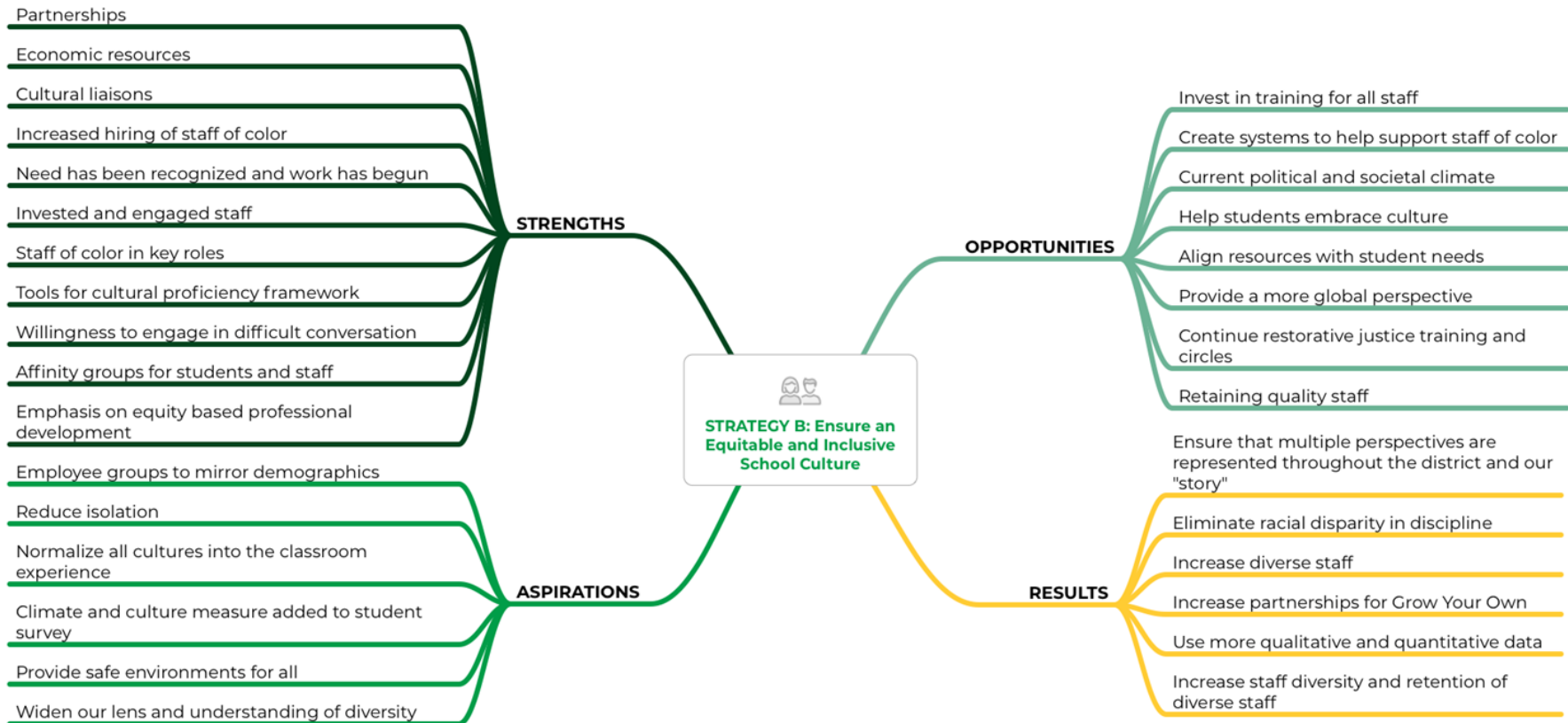


# STRATEGY A: Advance Academic Excellence, Growth and Readiness



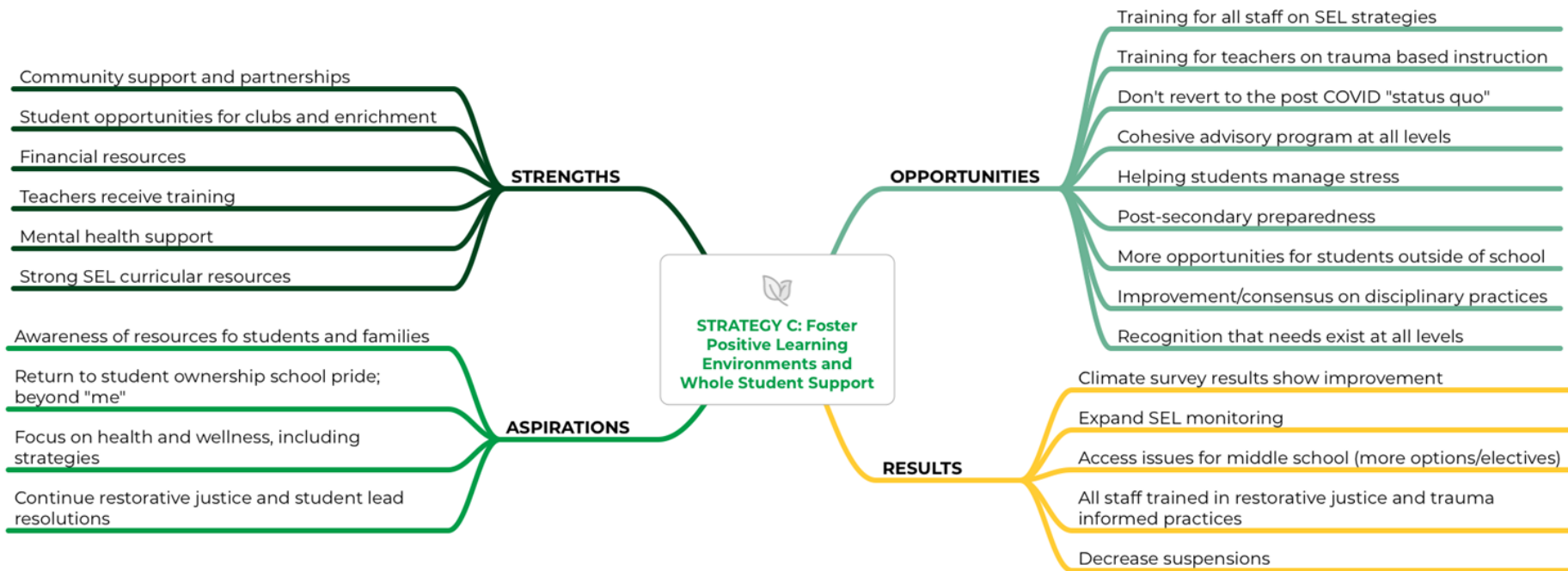


# STRATEGY B: Ensure an Equitable and Inclusive School Culture



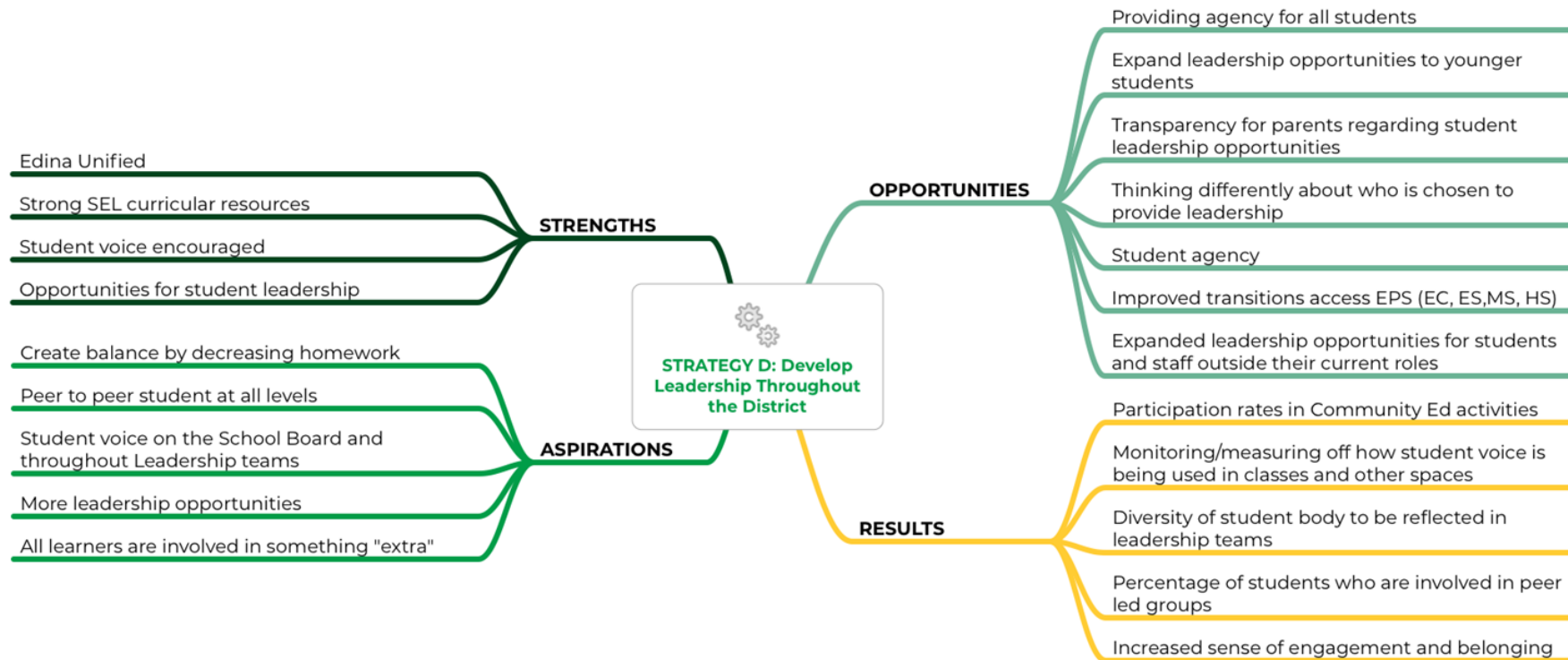


# STRATEGY C: Foster Positive Learning Environments and Whole Student Support



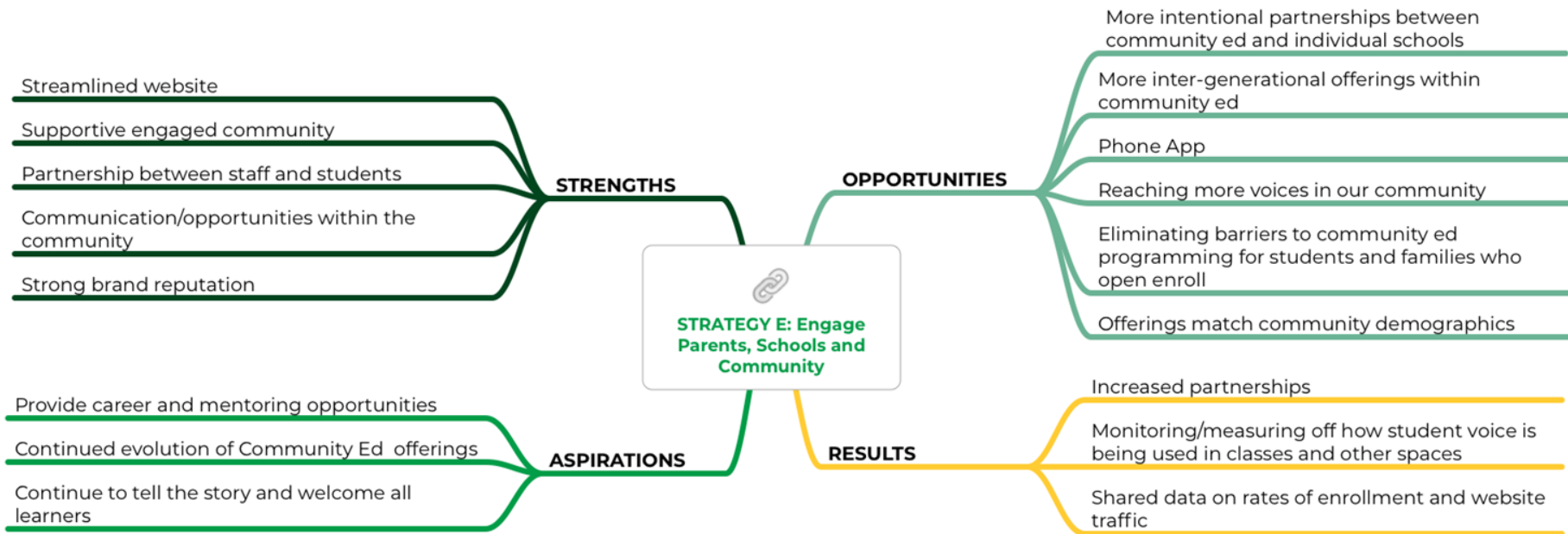


# STRATEGY D: Develop Leadership Throughout the District





# STRATEGY E: Engage Parents, Schools and Community





# Key Messages to the Community





# Key Messages to the Community

- This process was very intentional about including a wide variety of perspectives at the table, including centering student voice.
- We are very hopeful for the future of Edina Public Schools and look forward to continuing this critical work.
- We have much to celebrate in our district! While we know there is much work to be done, it's important to take time to recognize and celebrate the many amazing accomplishments that happen every day in our classrooms and throughout our district.
- The district is taking this work very seriously and cares deeply about input from the community.
- The implementation process will take time. There are concrete action steps behind the plan and district leadership is committed to including the community throughout the process.
- Attracting, retaining, and supporting a diverse group of staff is important to many stakeholders in our district.





# Thank You!





**Board Work Session: June 13, 2022**

**TITLE:** Panorama Student and Staff Data Presentation

**TYPE:** Discussion

**PRESENTER(S):** Dr. Randy Smasal, Assistant Superintendent

**BACKGROUND:** The Panorama Well-being and Engagement surveys were administered to Edina Public School students in grades 3-12 in the month of March 2022. To date, these surveys have been used in more than three thousand schools and with over two million students, family members, teachers and staff members across diverse geographic areas, school types, and achievement levels. This is the second year of utilization of the student surveys which has now helped to create a substantial baseline and second year of comparison. Our EPS scholars scored in the 80th to 99th %tiles nationally on the well being metrics and in the 50th to 70th %tiles for engagement. Specific quantitative student responses are included in this packet and qualitative summary responses to the open ended questions are included in the slide presentation.

Licensed staff (Administrators and Teachers) were asked to complete the School Climate survey prior to spring break, March 2022. This was the first time using the School Climate survey with staff and so this data provides a baseline metric moving forward. School Climate was ranked at the 10% tile nationally on cumulative norms for years prior to and during COVID. Specific quantitative staff responses are included in the packet below and a brief summary of qualitative responses to the open ended questions are in the slide deck.

Administrative plans for use of the data to improve student engagement and school climate will be discussed and are included with the attached information.

**RECOMMENDATION:**

- No recommendation is being made at this time.

**DESIRED OUTCOME FROM THE BOARD:**

- Review supporting documents and determine what questions you would like responses to and provide feedback you would like considered by administration

**ATTACHMENTS:**

- See attached [Slide Deck](#)
- See attachment of listing responses by question and group



# Panorama Results Update: Board Presentation

June 13, 2022

Dr. Randy Smasal



# Presentation Overview

- Survey Background
- Student Results
- Staff Results
- Next Steps



# Student Background Information:

- Survey of School Climate and Social Emotional Learning given to students in grades 3-12 and staff in grades K-12 using a survey tool from Panorama.
- Survey was first taken in March of 2021, and again in March of 2022 (two years of baseline data).
- Survey includes national norms comparing EPS with data from other schools across the country.
- National Benchmarks also include your approximate national percentile, rounded to the nearest 10 (e.g. 50th or 70th percentile).
- National Benchmarks include survey results from more than three thousand schools and two million students, family members, teachers and staff members across various geographic areas, school types, and achievement levels.



# Survey Results

- Student Results

- n=1414 for Gr. 3-5

- Grade 3-5 Enrollment = 1831 (77% completed survey)

- n=1775 for Gr. 6-12

- Grades 6-12 Enrollment = 4630 (38% completed survey)

- Staff Results (n=397)

- Licensed Staff at sites = 643 (62% completed survey)






# Student Results

Grade 3-5	2021 (Favorable)	National %tile ranking	2022 (Favorable)	National %tile ranking	Change
Supportive Relationships	89%	80th	91%	90th	↑
Positive Feelings	77%	90th	77%	90th	▬
Challenging Feelings	67%	99th	66%	99th	▬
Emotion Regulation	54%	90th	54%	90th	▬
Engagement	62%	80th	59%	70th	↓

Favorable means the percent of respondents selecting the top two likert scale response choices for questions in the category.



# Student Results

Grade 6-12	2021 (Favorable)	National %tile ranking	2022 (Favorable)	National %tile ranking	Change
Supportive Relationships	84%	80th	84%	80th	
Positive Feelings	67%	90th	66%	90th	
Challenging Feelings	60%	90th	63%	99th	
Emotion Regulation	51%	80th	52%	80th	
Engagement	23%	40th MS / 60th HS	28%	50th MS / 70th HS	



# Staff Results

	2022 (Favorable)	National %tile ranking
School Climate	40%	10th



# Spring 2022 Panorama

## 3rd - 5th grade





Thinking about everything in your life right now, what makes you feel the happiest? ?

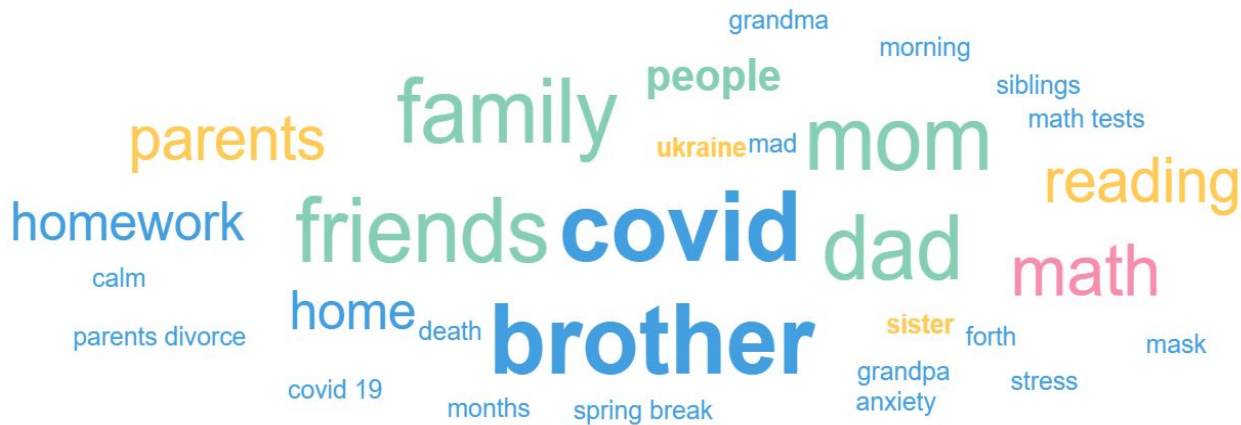
**Student Responses  
Gr. 3-5:**





Thinking about everything in your life right now, what feels the hardest for you? ?

Student  
Responses  
Gr. 3-5:

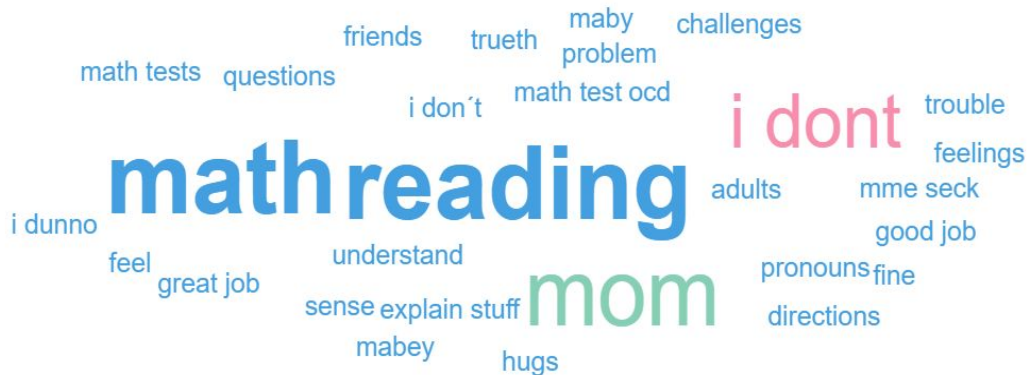




[< Summary](#)

## What can teachers or other adults at school do to better help you? ?

**Student Responses:  
Gr. 3-5**





# Spring 2022 Panorama

## 6th - 12th grade





Thinking about everything in your life right now, what makes you feel the happiest? ?

Student  
Responses  
6-12





Thinking about everything in your life right now, what feels the hardest for you? ?

Student  
Responses  
6-12





< Home

**District**

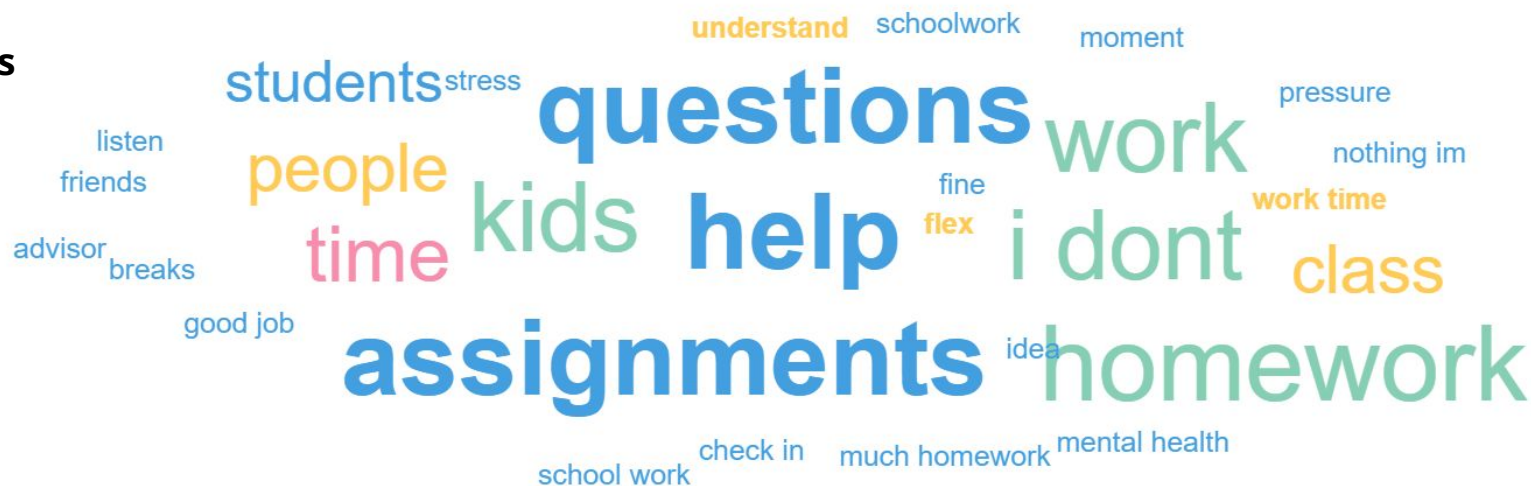
Schools

Comparisons

Response Rates

## What can teachers or other adults at school do to better support you? ?

**Student  
Responses  
6-12**





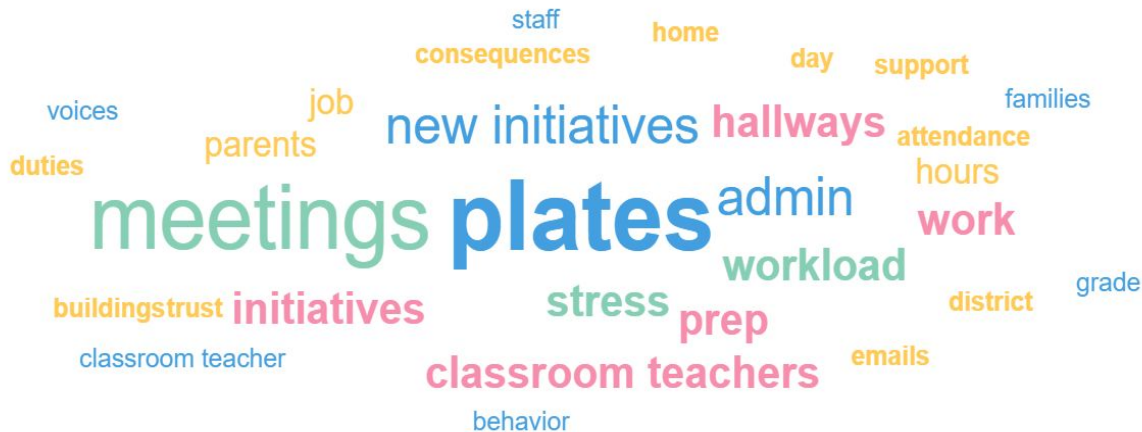
# Spring 2022 Panorama Staff





Understanding that time is often of the greatest concern, what else would most help you manage your current stress level? ?

Staff  
Responses:





# Key Findings



# Students: Key Findings

- All Gr. 3-5 students ratings in for well being in 90th-99th percentile nationally.
- All Gr. 6-12 student ratings for well being in 80th-99th percentile nationally.
- Gr. 3-5 Edina Virtual Pathway had comparable high ratings for the well being measures.
- Gr. 3-5 students reported lower engagement ratings than the previous year, moving from the 80th percentile to the 70th percentile nationally.
- Gr. 6-12 students reported higher engagement ratings than the previous year, from:
  - 40th percentile to the 50th percentile in Middle School
  - 60th percentile to the 70th percentile in High School



# Staff Results: Key Findings Regarding Climate

Baseline Rating 40% Favorable Responses (10th percentile)

## Low Ratings:

- Attitudes of Colleagues
- Support for Initiatives
- Working Environment
- Optimism for Improvement
- Support of Students for Each Other

## Moderate Ratings:

- Enthusiasm of Students
- Staff trusted in their work
- Respectful Relationships between staff and students



# Staff Results: Key Findings Regarding Climate

## Open Ended Responses:

- Student social and academic skills were negatively impacted by COVID; significant increase in behavior issues
- More support needed for learners
- Exhausted
- Plates are overflowing
- Staff morale suffered
- New initiatives were challenging
- Desire for greater input on decisions
- Reexamine the substitute model
- Enhance communication with staff



## Panorama Playbook

# Explore strategies for taking action

Engage with hundreds of research-backed SEL interventions, activities and resources from expert organizations to improve your practice. Browse Playbook's partners and topics below.

[Adult SEL](#)

[Better Kids](#)

[Conscious  
Discipline](#)

[Distance  
Learning](#)

[Emotion  
Regulation](#)

[Engagement](#)

[Equity &  
Inclusion](#)

[Everyday  
Speech](#)

[Family  
Engagement](#)

[Growth Mindset](#)

[Open Circle](#)

[Peekapak](#)

[Playworks](#)

[QuaverEd](#)

[Respectful Ways](#)

[Rigorous  
Expectations](#)

[School and  
Classroom  
Climate](#)

[Second Step](#)

[Self-Efficacy](#)

[Self-  
Management](#)

[Sense of  
Belonging](#)

[Social  
Awareness](#)

[Take 5! Institute](#)

[Teacher Growth  
Mindset](#)

[Teacher-Student  
Relationships](#)



# Next Steps



# District and Site Next Steps

## Summer 2022

- Training for all admin and site leadership teams on accessing the playbook in Panorama based upon their specific site level data
  - Each site leadership team will meet with the team from Panorama to review student and staff data and playbook intervention recommendations.
  - A particular focus will be on engagement strategies

## August 2022

- Training for all admin and site leadership teams on Leading Change
  - Increase ability of site leadership teams to apply effective change strategies

## June - July 2022

- Review the Substitute System for the 22-23 school year
  - Examine budget and capability to blend Premier, On call and Virtual sub models



# District and Site Next Steps

- Each site will include climate improvement goals and action plans in their school improvement plan (Due September 2022)
  - Actions plans (developed by admin and EME reps) are already in development. Examples include:
    - Community building activities with staff
    - Monthly connect meetings with EME and other bargaining group representatives
    - ML teachers to meet with teams more regularly in secondary schools. ML training will be a focus in secondary schools in 22-23.
  - Fall 2022: All admin, teachers and support staff to be proficient in the use of the language line.
- District Admin to meet monthly with principals to review school site improvement plan progress



**Thank you**  
**What questions do you have?**





# Edina Public School District

Grades 3-5  
School and Climate Survey 2022







Report created by  
Panorama Education





## Summary

Topic Description	Results	Benchmark
<b>Challenging Feelings</b> How frequently students feel challenging emotions, with higher scores indicating less frequent challenging emotions.	<b>66%</b> ▼ 1 since last survey	 80th - 99th percentile compared to others nationally
<b>Emotion Regulation</b> How well students regulate their emotions.	<b>54%</b> 0 since last survey	 80th - 99th percentile compared to others nationally
<b>Positive Feelings</b> How frequently students feel positive emotions.	<b>77%</b> 0 since last survey	 80th - 99th percentile compared to others nationally
<b>Supportive Relationships</b> How supported students feel through their relationships with friends, family, and adults at school.	<b>91%</b> ▲ 2 since last survey	 80th - 99th percentile compared to others nationally

1,414 responses





## Challenging Feelings

Your average

**66%**

1,414 responses

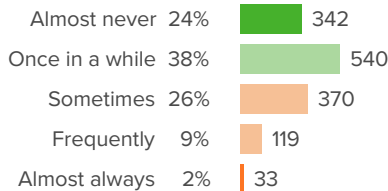
Change

▼ **1**

since last survey

How did people respond?

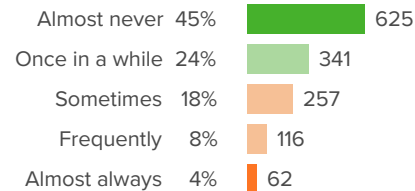
**Q.1: During the past week, how often did you feel mad?**



▼ **2** from last survey

Favorable: **63%**

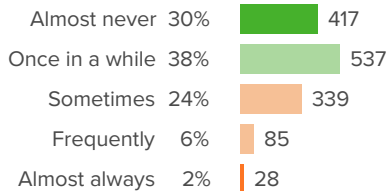
**Q.2: During the past week, how often did you feel lonely?**



▲ **1** from last survey

Favorable: **69%**

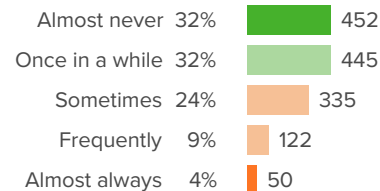
**Q.3: During the past week, how often did you feel sad?**



▼ **1** from last survey

Favorable: **68%**

**Q.4: During the past week, how often did you feel worried?**



▲ **0** from last survey

Favorable: **64%**





## Emotion Regulation

Your average

**54%**

1,414 responses

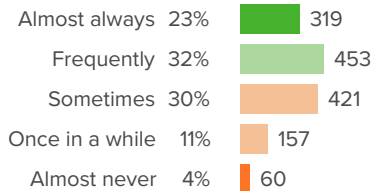
Change

**0**

since last survey

How did people respond?

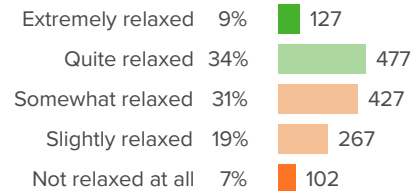
**Q.1: How often are you able to pull yourself out of a bad mood?**



▼ 1 from last survey

Favorable: **55%**

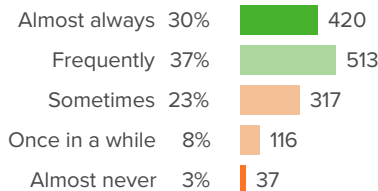
**Q.2: When everybody around you gets angry, how relaxed can you stay?**



▲ 1 from last survey

Favorable: **43%**

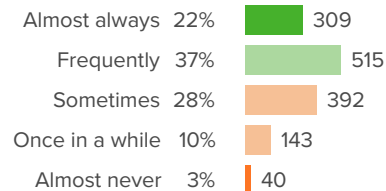
**Q.3: How often are you able to control your emotions when you need to?**



▼ 1 from last survey

Favorable: **67%**

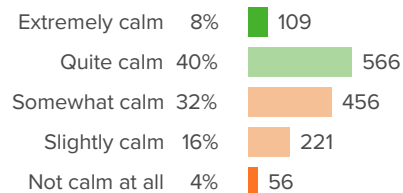
**Q.4: Once you get upset, how often can you get yourself to relax?**



▼ 1 from last survey

Favorable: **59%**

**Q.5: When things go wrong for you, how calm are you able to stay?**



▲ 2 from last survey

Favorable: **48%**





## Positive Feelings

Your average

**77%**

1,414 responses

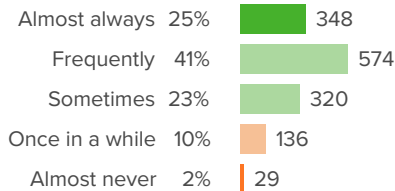
Change

**0**

since last survey

### How did people respond?

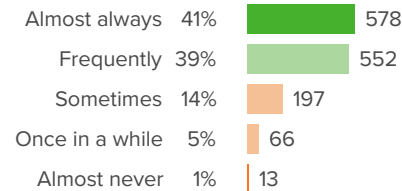
#### Q.1: During the past week, how often did you feel excited?



▲ 0 from last survey

Favorable: **88%**

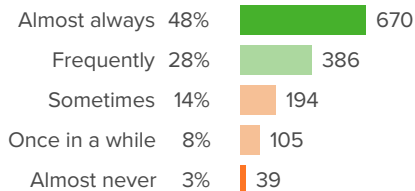
#### Q.2: During the past week, how often did you feel happy?



▲ 1 from last survey

Favorable: **80%**

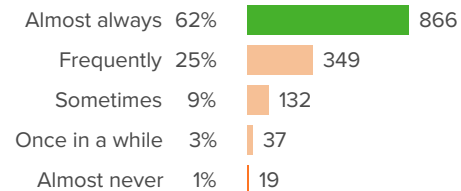
#### Q.3: During the past week, how often did you feel loved?



▲ 2 from last survey

Favorable: **76%**

#### Q.4: During the past week, how often did you feel safe?



▼ 4 from last survey

Favorable: **62%**





## Supportive Relationships

Your average

91%

1,414 responses

Change

▲ 2

since last survey

How did people respond?

**Q.1: Do you have a teacher or other adult from school who you can count on to help you, no matter what?**

Yes	88%	<div></div>	1228
No	12%	<div></div>	173

▲ 1 from last survey

Favorable: 88%

**Q.2: Do you have a family member or other adult outside of school who you can count on to help you, no matter what?**

Yes	95%	<div></div>	1331
No	5%	<div></div>	66

▲ 0 from last survey

Favorable: 95%

**Q.3: Do you have a friend from school who you can count on to help you, no matter what?**

Yes	89%	<div></div>	1242
No	11%	<div></div>	158

▲ 4 from last survey

Favorable: 89%





# Edina Public School District

Grades 3-5  
School and Climate Survey 2022




Report created by  
Panorama Education





## Summary

Topic Description	Results	Benchmark
<b>Engagement</b> How attentive and invested students are in class.	<b>59%</b> ▼ 3 since last survey	 60th - 79th percentile compared to others nationally

1,349 responses





## Engagement

Your average

**59%**

1,349 responses

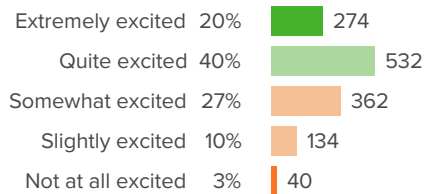
Change

▼ **3**

since last survey

How did people respond?

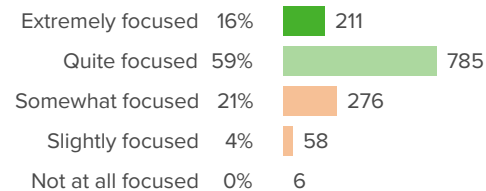
### Q.1: How excited are you about going to this class?



▼ **6** from last survey

Favorable: **60%**

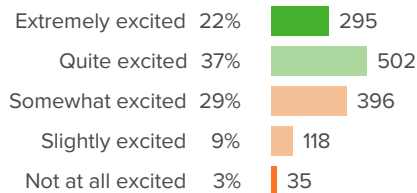
### Q.2: How focused are you on the activities in this class?



▲ **0** from last survey

Favorable: **75%**

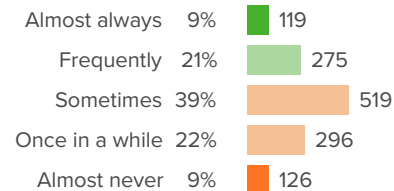
### Q.3: In this class, how excited are you to participate?



▼ **2** from last survey

Favorable: **59%**

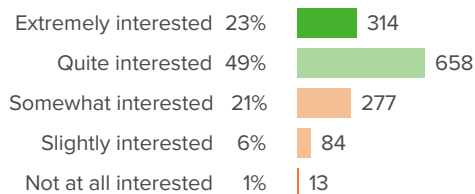
### Q.4: When you are not in school, how often do you talk about ideas from this class?



▼ **2** from last survey

Favorable: **30%**

### Q.5: How interested are you in this class?



▼ **2** from last survey

Favorable: **72%**





# Edina Public School District

Grades 6-12  
School and Climate Survey 2022



Report created by  
Panorama Education





## Summary

Topic Description	Results	Benchmark
<b>Challenging Feelings</b> How frequently students feel challenging emotions, with higher scores indicating less frequent challenging emotions.	<b>63%</b> ▲3 since last survey	 80th - 99th percentile compared to others nationally
<b>Emotion Regulation</b> How well students regulate their emotions.	<b>52%</b> ▲1 since last survey	 80th - 99th percentile compared to others nationally
<b>Positive Feelings</b> How frequently students feel positive emotions.	<b>66%</b> ▼1 since last survey	 80th - 99th percentile compared to others nationally
<b>Supportive Relationships</b> How supported students feel through their relationships with friends, family, and adults at school.	<b>84%</b> 0 since last survey	 60th - 79th percentile compared to others nationally

1,775 responses





## Challenging Feelings

Your average

**63%**

1,775 responses

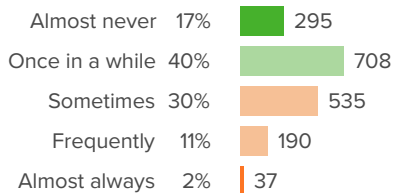
Change

**▲ 3**

since last survey

How did people respond?

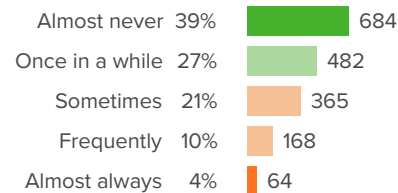
**Q.1: During the past week, how often did you feel angry?**



▲ 0 from last survey

Favorable: **57%**

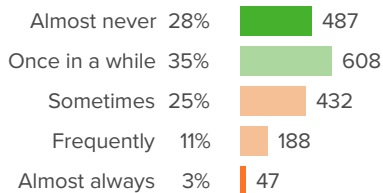
**Q.2: During the past week, how often did you feel lonely?**



▲ 5 from last survey

Favorable: **66%**

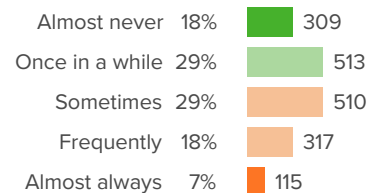
**Q.3: During the past week, how often did you feel sad?**



▲ 3 from last survey

Favorable: **62%**

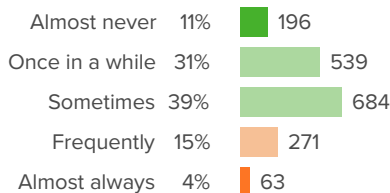
**Q.4: During the past week, how often did you feel worried?**



▲ 5 from last survey

Favorable: **47%**

**Q.5: During the past week, how often did you feel frustrated?**



▲ 2 from last survey

Favorable: **81%**





## Emotion Regulation

Your average

**52%**

1,775 responses

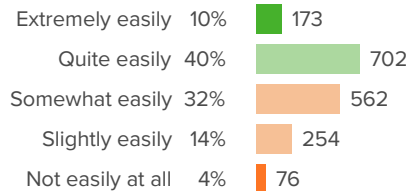
Change

**▲ 1**

since last survey

How did people respond?

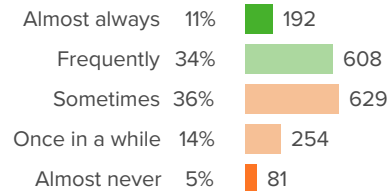
**Q.1: When you are feeling pressured, how easily can you stay in control?**



▲ 5 from last survey

Favorable: **50%**

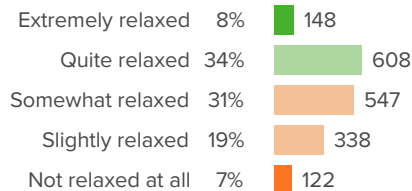
**Q.2: How often are you able to pull yourself out of a bad mood?**



▼ 2 from last survey

Favorable: **45%**

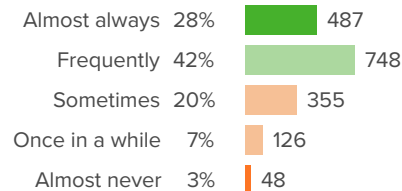
**Q.3: When everybody around you gets angry, how relaxed can you stay?**



▲ 0 from last survey

Favorable: **43%**

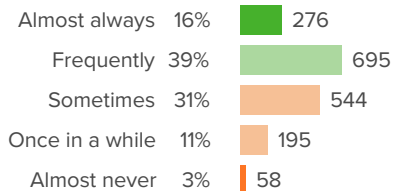
**Q.4: How often are you able to control your emotions when you need to?**



▼ 3 from last survey

Favorable: **70%**

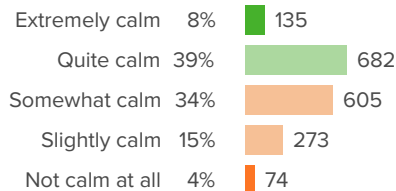
**Q.5: Once you get upset, how often can you get yourself to relax?**



▲ 0 from last survey

Favorable: **55%**

**Q.6: When things go wrong for you, how calm are you able to remain?**



▲ 4 from last survey

Favorable: **46%**





## Positive Feelings

Your average

**66%**

1,775 responses

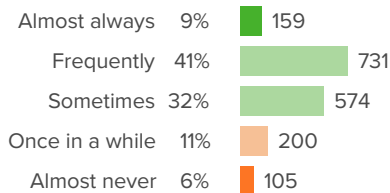
Change

▼ **1**

since last survey

How did people respond?

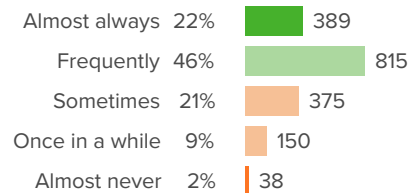
**Q.1: During the past week, how often did you feel excited?**



▲ **5** from last survey

Favorable: **83%**

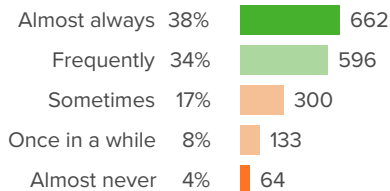
**Q.2: During the past week, how often did you feel happy?**



▲ **2** from last survey

Favorable: **68%**

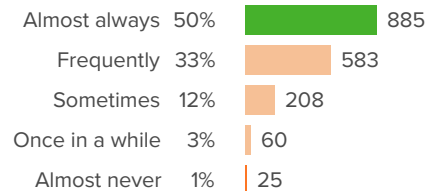
**Q.3: During the past week, how often did you feel loved?**



▼ **4** from last survey

Favorable: **72%**

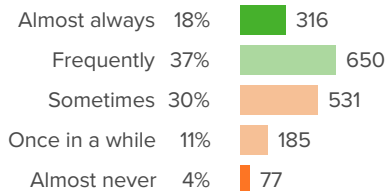
**Q.4: During the past week, how often did you feel safe?**



▼ **8** from last survey

Favorable: **50%**

**Q.5: During the past week, how often did you feel hopeful?**



▲ **0** from last survey

Favorable: **55%**





## Supportive Relationships

Your average

**84%**

1,775 responses

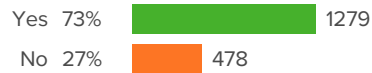
Change

**0**

since last survey

How did people respond?

**Q.1: Do you have a teacher or other adult from school who you can count on to help you, no matter what?**



▲ 0 from last survey

Favorable: **73%**

**Q.2: Do you have a family member or other adult outside of school who you can count on to help you, no matter what?**



▲ 0 from last survey

Favorable: **94%**

**Q.3: Do you have a friend from school who you can count on to help you, no matter what?**



▲ 1 from last survey

Favorable: **90%**

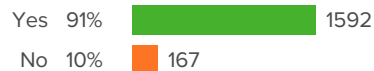
**Q.4: Do you have a teacher or other adult from school who you can be completely yourself around?**



▲ 1 from last survey

Favorable: **65%**

**Q.5: Do you have a family member or other adult outside of school who you can be completely yourself around?**



▲ 0 from last survey

Favorable: **91%**

**Q.6: Do you have a friend from school who you can be completely yourself around?**



▲ 1 from last survey

Favorable: **93%**





# Edina Public School District

Grades 6-12  
School and Climate Survey 2022




Report created by  
Panorama Education





## Summary

Topic Description	Results	Benchmark
<b>Engagement</b> How attentive and invested students are in class.	<b>28%</b> ▲ 5 since last survey	 0th - 19th percentile compared to others nationally

1,641 responses





## Engagement

Your average

**28%**

1,641 responses

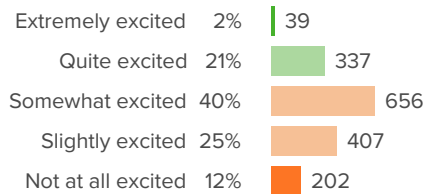
Change

**▲ 5**

since last survey

### How did people respond?

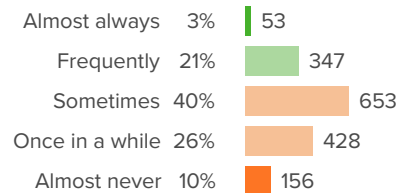
#### Q.1: How excited are you about going to your classes?



▲ 5 from last survey

Favorable: **23%**

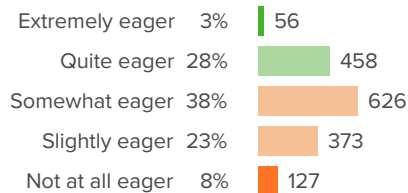
#### Q.2: How often do you get so focused on activities in your classes that you lose track of time?



▲ 5 from last survey

Favorable: **24%**

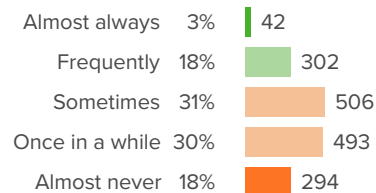
#### Q.3: In your classes, how eager are you to participate?



▲ 7 from last survey

Favorable: **31%**

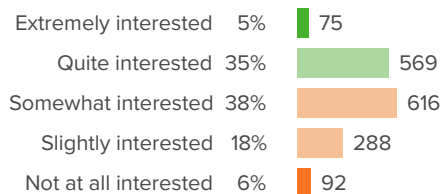
#### Q.4: When you are not in school, how often do you talk about ideas from your classes?



▲ 3 from last survey

Favorable: **21%**

#### Q.5: Overall, how interested are you in your classes?



▲ 5 from last survey

Favorable: **39%**





# Edina Public School District

Staff Survey  
School and Climate Survey 2022




Report created by  
Panorama Education





## Summary

Topic Description	Results	Benchmark
<b>School Climate</b> Perceptions of the overall social and learning climate of the school.	<b>40%</b>	 0th - 19th percentile compared to others nationally

397 responses





# School Climate

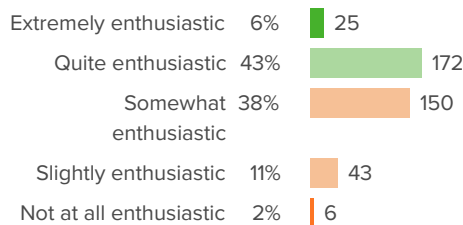
Your average

40%

397 responses

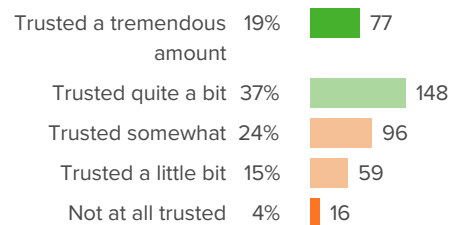
How did people respond?

**Q.1: On most days, how enthusiastic are the students about being at school?**



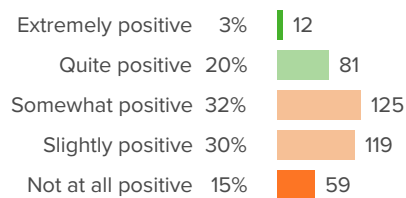
Favorable: **50%**

**Q.2: To what extent are staff trusted to work in the way they think is best?**



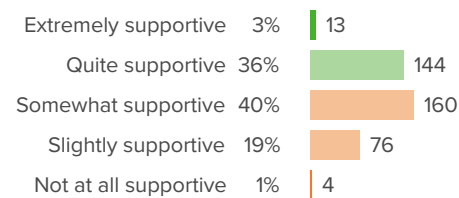
Favorable: **57%**

**Q.3: How positive are the attitudes of your colleagues?**



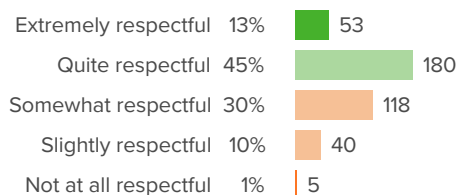
Favorable: **23%**

**Q.4: How supportive are students in their interactions with each other?**



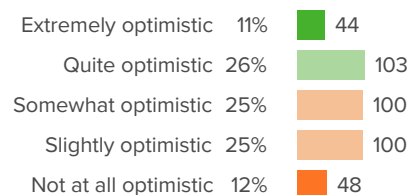
Favorable: **40%**

**Q.5: How respectful are the relationships between staff and students?**



Favorable: **59%**

**Q.6: How optimistic are you that your school will improve in the future?**

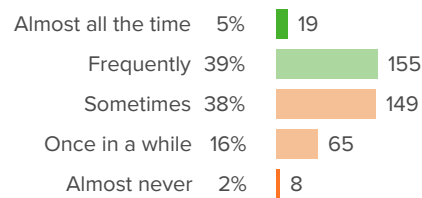


Favorable: **37%**



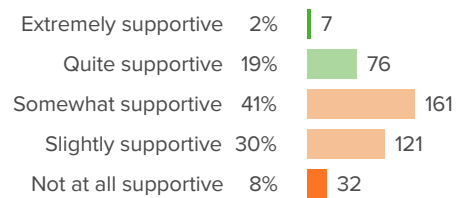


**Q.7: How often do you see students helping each other without being prompted?**



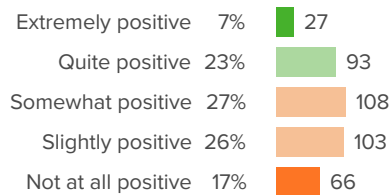
Favorable: **44%**

**Q.8: When new initiatives are presented at your school, how supportive are your colleagues?**



Favorable: **21%**

**Q.9: Overall, how positive is the working environment at your school?**



Favorable: **30%**





**Board Meeting Date: June 13, 2022**

**TITLE:** Edina Virtual Pathway Update

**TYPE:** Discussion

**PRESENTER(S):** Steven Cullison, Edina Virtual Pathway Coordinator; Natasha Monsaas-Daly, Director of Media and Technology Services; Jody De St. Hubert, Director of Teaching and Learning; and Michael Walker, Digital Learning Specialist

**BACKGROUND:** In the Spring of 2021 the Edina Public Schools School Board approved further development of virtual pathways in alignment with the Edina Strategic Plan. Nearly 100 students have been enrolled in the comprehensive K-6 Edina Virtual Pathway (EVP) during the 2021-22 school year. The program was developed in the summer of 2021 in response to family interest and quickly grew from two sections to five. In addition 14 online supplemental sections were offered at Edina High School in 2021-22. These sections were taken as part of a student's full schedule in which most of their classes were in person. A design team at each level has been engaging in continued development of a K-12 Edina Virtual Pathway. On March 14th the team presented an update to the School Board. The attached report provides an update on the planning process since March 14th.

**RECOMMENDATION:** The purpose of this report is to update the board and have a discussion on the current Edina Virtual Pathway progress.

**DESIRED OUTCOMES FOR THE BOARD:** Review in detail, have questions prepared, and provide feedback on program development.

**ATTACHMENTS:**

1. Edina Virtual Pathway Report

**APPENDICES:**

- [March 14 Board Workshop Report](#)
- EVP [Website](#)



## **Edina Virtual Pathway Purpose:**

The Edina Virtual Pathway was developed for the 2021-22 school year because of the demand for a virtual offering from families with students enrolled in Edina Public Schools. The reason for expanding beyond the current programming to a fully operated comprehensive K-12 online school is due to the success of the current programming and the continued demand to provide learning choice opportunities from Edina families outlined in the 2020-2025 Strategic Plan. In order to fully fund a comprehensive K-12 online pathway, revenue must be generated. This revenue will be generated from student enrollment that captures students throughout the state of MN who would thrive with the enriching opportunities provided in an Edina education and from Edina residents who are currently accessing other school options.

*Defining Excellence:* Online programs have long offered flexible options for students that learn better in a different environment or at a different pace. It was a niche product accessed by some, but not many students. Since the pandemic there has been a marked increase in the interest of online options across the state. There are currently 61 state approved online providers. By offering an online option - Virtual Pathway - Edina Public Schools will remain positioned to define excellence in this expanding option.

*Retain and Draw Students:* Developing an online option in our district will allow us to retain those students that might otherwise enroll in online programs that are offered at neighboring districts, or from private curriculum providers. Provided the option to remain connected with the quality instruction that Edina's teachers offer, we believe our students will make the choice to remain an Edina student. As a state approved provider we are also able to offer the excellence of Edina schools to students across the state. Drawing students to enroll from anywhere in the state of Minnesota will help to pay for the program, and has the potential to support our neighborhood schools by generating additional revenue for specialized programs.

*Innovate and Elevate:* Online programs provide a unique opportunity to explore cutting edge ways to explore and learn. Removing the restrictions of time and place will inform new methods for learning that can also be explored in our physical school buildings.

*Discover Possibilities and Thrive:* There is a group of students, some student athletes, some entrepreneurs, some with health concerns and some just better served by a more flexible and independent option that we are not currently able to serve across our system. By expanding the settings and options for academic learning we extend our ability to truly meet the needs of all students.



## **What Sets Edina Virtual Pathway Apart?**

As the Edina Virtual Pathway develops there are established program components that set it apart from other online programs. These components are:

1. Balance
2. Small Groups and Personalized Learning
3. Passion Aligned
4. Growing and Critical Collaboration with the Excellence of Edina Staff

At our May 12th Board Meeting we were able to witness the excellence of Edina staff first hand when our Elementary Team presented during the Excellence in Action portion of the meeting. In addition to the commitment and skill that was demonstrated by our elementary staff on May 12th, our secondary staff have gone above and beyond as they collaborate and plan for the next level of EVP development in grades 6-12. Finally, in May our new EVP Coordinator Steven Cullison was hired. Steven previously served as a teacher at Edina High School. During the last month of the school year he contributed to ongoing EVP work alongside his teaching duties and is now solely focusing on the continued development of Edina Virtual Pathways.

## **Edina Virtual Pathway Updates Since March:**

1. Comprehensive Approval for K-12
2. Enrollment Open K-12
  - a. Continuing to monitor enrollment numbers weekly with Cabinet in collaboration with our enrollment center staff
  - b. Adjusted and lowered enrollment goals
    1. Elementary : 5 sections
    2. Middle school: 60 total (20 per grade level)
    3. High School: 80 total (20 per grade level)
3. Marketing and Communications
  - a. Updated Website
  - b. Contacted all families who had expressed interest via email and phone
  - c. Contacted all homeschool families
  - d. Newspaper ads developed
4. MOU Impact for HS Online
  - a. MOU offering has increased the number of sections offered by 19 so far
  - b. Structure for adding additional Supplemental Students developed
5. Professional Development
  - a. Secondary EVP professional development opened June 8th
  - b. Elementary professional development to be scheduled

## **Enrollment:**

Edina Virtual Pathway enrollment is currently mirroring the enrollment at this time in 2021 with approximately 50 students enrolled. Through daily enrollment updates the administration team



is able to monitor patterns and prepare for a continued summer increase in enrollment. This summer enrollment increase is not only what Edina directly experienced in 2021 but also what surrounding established virtual schools have experienced over multiple years of enrollment.

## Guiding Change Document: K-12 Edina Virtual Pathways

GUIDING CHANGE DOCUMENT: K-12 Edina Virtual Pathways		
Context and Reality <i>"The Why"</i>	Unacceptable Means <i>"The Not-How"</i>	Results <i>"The What"</i>
<ul style="list-style-type: none"> <li>• Our charge is to educate all at high levels of engagement and rigor.</li> <li>• Virtual Pathways align with our 2020-25 Strategic Plan goal strategy A to provide a coherent and differentiated educational experience by articulating a system of flexible pathways that maximize students strengths and talents.</li> <li>• A Virtual Pathway experience exposes students to Future Ready competencies.</li> <li>• Our Edina Learning Framework includes many components that online learning addresses, such as: Anytime/Anywhere learning, Flexible Learning Spaces, Digital Age learning, Student Voice and Choice, Proficiency-based learning and assessment.</li> <li>• Students have been accessing online instruction at the secondary level for over 20 years.</li> <li>• The number of online learning providers in Minnesota has expanded from a handful to over 60 this year, with the potential for a 50% increase next year.</li> <li>• Edina currently has over 400 secondary students taking online courses supplementally at Northern Star Online, as well as other providers.</li> <li>• Edina families left Edina Schools this past year seeking a comprehensive online experience elsewhere.</li> <li>• During distance learning, Edina students and families appreciated the</li> </ul>	<ul style="list-style-type: none"> <li>• Create additional inequities in services among schools and programs that result in opportunity gaps.</li> <li>• Develop educational goals, services and programs that are not coherent or consistent with the Edina Public Schools strategic plan, mission, vision, and/or values.</li> <li>• Exceed facility or grade level capacities.</li> <li>• Exceed available funding limits.</li> <li>• Recommendations developed without periodic school board updates.</li> <li>• The rate of growth is too fast and not aligned with school board expectations.</li> <li>• Negative impact on students in our traditional schools.</li> <li>• Negative impact on course offerings or staffing in our existing buildings.</li> <li>• Negative impact on extracurricular opportunities for students in our existing buildings.</li> <li>• Developing a system that does not support all learners' needs</li> <li>• Implementing a online program that does not adequately support members of that community (learners, families, teaching staff, administrative staff) in aligning with our mission, vision and/or values</li> </ul>	<ul style="list-style-type: none"> <li>• The Edina Virtual Pathway K-12 expands and improves, and becomes a stand-alone school in our system.</li> <li>• Edina High School students are able to take Edina Virtual Pathway 9-12 courses supplementally.</li> <li>• All online students are Career, Civic, College, and Future Ready when they leave the system.</li> <li>• Every student meets or exceeds proficiency and growth targets.</li> <li>• Student engagement is maximized.</li> <li>• Parental Engagement is maximized.</li> <li>• School leadership is supported in implementing all components of the online pathway</li> <li>• School and district leadership maintains a strong collaboration that honors unique building and online program needs.</li> <li>• All staff are highly knowledgeable in how children learn in an online environment.</li> <li>• Staff's impact on online instruction is maximized through data-driven, job-embedded professional development on evidence-based instruction.</li> </ul>



<p>flexibility that online learning provided.</p> <ul style="list-style-type: none"> <li>• Positive feedback has been gathered from our students and families around Virtual Pathways currently offered.</li> <li>• As a state-approved provider, we are also able to offer the excellence of Edina schools to students across the state. Drawing students to enroll from anywhere in the State of Minnesota will help to pay for the program, and has the potential to support our neighborhood schools by generating additional revenue for specialized programs.</li> </ul>		<ul style="list-style-type: none"> <li>• Support staff's impact on online instruction is maximized.</li> <li>• A multi-tiered system of academic and social-emotional support is in place for all learners.</li> <li>• Students know and are known by their peers and instructors.</li> <li>• Instruction is personalized for all students and inclusive of a strengths-based mindset.</li> <li>• Rigorous course content and opportunities for advanced coursework are available.</li> <li>• Technology is leveraged and embedded as a tool to accelerate and enhance learning.</li> <li>• Edina Virtual Pathway is an incubator for innovation within the district.</li> </ul>
--	--	--





**Board Meeting Date:** 06/13/2022

**TITLE:** 2021-2022 Technology Report

**TYPE:** Discussion/Report

**PRESENTER(S):** Natasha Monsaas-Daly, Director, District Media & Technology Services

**BACKGROUND:** Strategy C.6 of EPS Strategic Plan tasks the district with completing a comprehensive review of technology used by staff and students. An outcome of this objective would be for the district to adopt an updated technology plan.

Year one of development of this plan was focused on an audit of our current systems, processes, and needs. This report reflects the findings of this audit, as well as next steps.

**RECOMMENDATION:** This report is for information and discussion.

**PRIMARY ISSUE(S) TO CONSIDER:** None

**ATTACHMENTS:**

1. Report (next page)
2. Presentation



## Introduction

To know where we want to go, it is critical to know where we are. In order to meet our strategic objectives, especially Strategy C.6, it was imperative for DMTS to take time this year to conduct an audit of our technology systems. Our work this year is the first step in a phased approach in the development of a long-range technology plan. The [current district technology plan](#) was last revised in 2014. In addition to creating a new plan, we will also determine a process for annual review of the plan.

To begin, it was important to understand our current technology landscape, as well as the individuals impacted by each of our systems. The shift to distance learning during the 2020-2021 school year, put a pause on our work to upgrade our digital classroom standards across the district. Through this initial audit, we have been able to map out a three year plan to get our classrooms up to standard.

Covid also introduced an influx of new technologies to our classrooms. As such, beginning this audit has enabled us to bring in the necessary tools and procedures to monitor our classroom technology, create a more robust process for requesting new technology, and ensure all technology meets data privacy standards. Our most important and expansive project in the upcoming years will likely be in the area of cybersecurity. While cyber insurance requirements are more stringent, we know the threat against our systems is increasing. Over the next several years, the board should plan to see an increased effort, both financially and procedurally, towards increasing our security posture.

This report will focus on the following areas:

- Digital Classroom Standards and Instruction: Instructional technology hardware and software used in the classroom.
- Cybersecurity Landscape: Our increased emphasis on updating our cybersecurity posture.
- Technology Skills: Creating an environment where students and staff are able to learn and obtain the necessary technology skills for the future.
- Where we are headed: As we audit our environment, we are also looking ahead and planning for future technology needs, changes, and upgrades.

## Our Current Environment

The Department of Media and Technology manages technology for thousands of staff and students. Staff may include vendors and contractors with access to various systems. In addition to human capital, we also maintain and manage a wide variety of technology. Many of these items are difficult to document in this report. Approximately 170 software tools have been approved for student use. Yet, this list does not include the tools needed for the district to function, such as our HR resources, finance resources, special education resources, etc. The table below provides a brief snapshot of our environment.

Brief Snapshot of our Service Environment	
Community	Total
Staff	~ 1975
Students	~ 8400
Technology	Quantity
Staff devices (laptops or desktops)	1,428



Student Chromebooks	6,410
Student iPads	2,421
Servers	94
Phones	1100
Wireless Access Points	550
Projectors	250
Interactive Whiteboards	230
Classroom Audio	300
Approved Student Tools	~ 170

## Digital Classroom Standards and Instruction

Central to our technology environment is the impact on classroom instruction. To ensure rigorous and authentic learning opportunities for all students, it is critical that our infrastructure and resources match those needs. This comes into play in two areas - the classroom environment and the tools provided to deliver instruction.

Currently, we have:

- 1:1 Devices. During the 2021-22 year, the pandemic escalated our move to 1:1 devices at all levels. Heading into the 2022-23 year, all K-1 students will be 1:1 with iPads. Grades 2-8 will be 1:1 with district-owned Chromebooks. Grades 9-12 will continue the hybrid bring-your-own-device (BYOD) model in partnership with Best Buy. This equitable access to technology is necessary for teachers to continue to *“Provide a coherent and differentiated educational experience that effectively engages, appropriately challenges every student academically”* (Edina Public Schools Strategic Priority A.2).
- The vast majority of our elementary classrooms received a classroom projection upgrade at the start of the pandemic. Most **elementary** classrooms are outfitted with a Viewsonic Interactive Panel. Our **secondary** classrooms generally have a projector in each room. This may vary depending upon classroom size or purpose.

This year, we evaluated our digital classroom standards across the district. This evaluation looked at the impact of classroom audio, classroom video, and teacher devices. Overwhelming, two areas of need stood out at the secondary level: classroom audio and classroom video. At the elementary level, the largest need centered in classroom audio.

Through this evaluation, we were able to develop and budget for a 3-year digital classroom standards upgrade. This will allow us to refresh critical classroom technologies in all of our schools. We will continue to monitor other technology needs, including staff devices in the coming years. Beginning with the 2022-23 school year, we will start our three year refresh process by upgrading projection and audio districtwide. Our main focus is on secondary classrooms, as elementary classrooms received a panel refresh in 2020 or 2021.

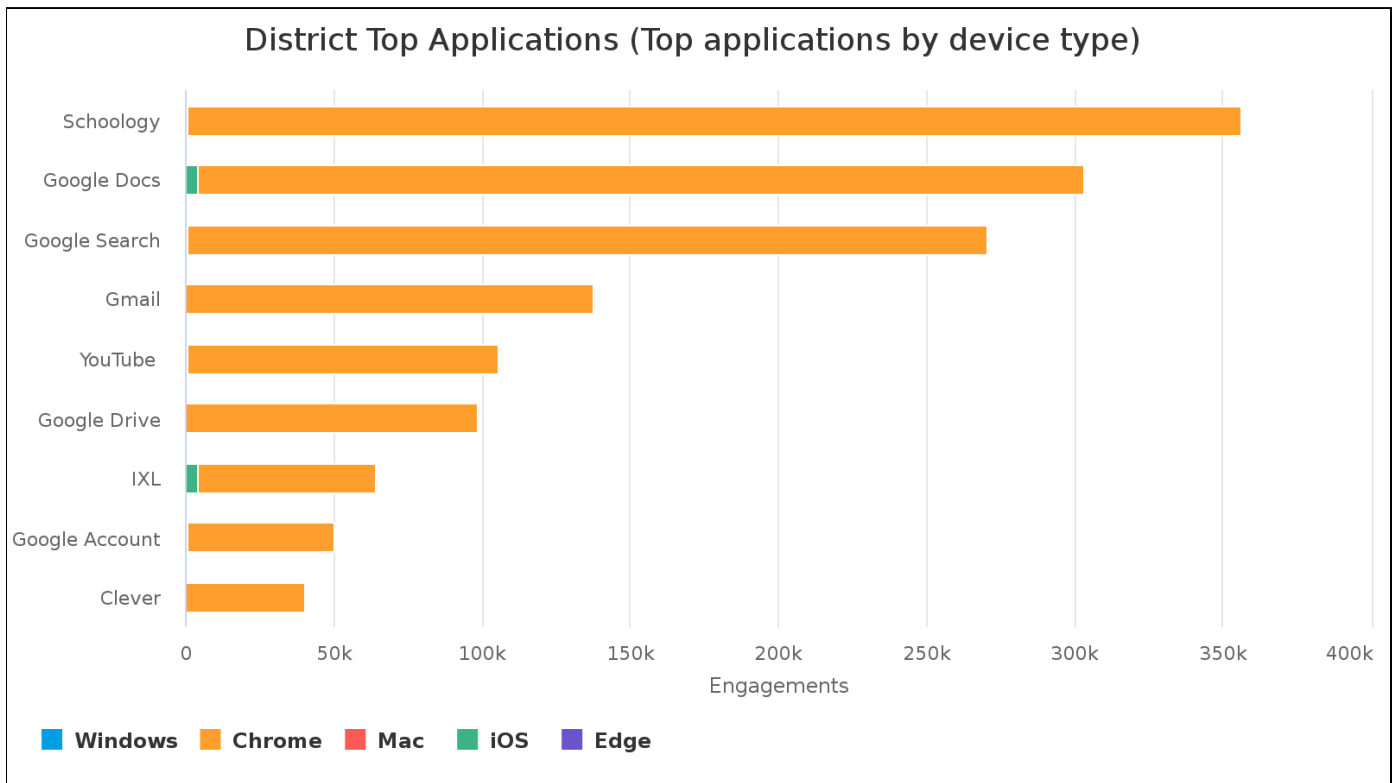


3-Year Digital Classroom Standards Update		
Timeline	Project Scope	Approximate Cost
Fall of 2022	<ul style="list-style-type: none"> <li>Upgrade video/projection at EHS</li> <li>Upgrade audio at SV &amp; VV</li> <li>Upgrade audio at ND</li> </ul>	\$265,000
Fall of 2023	<ul style="list-style-type: none"> <li>Upgrade audio at EHS</li> <li>Upgrade video/projection at SV &amp; VV</li> <li>Upgrade audio at CS</li> <li>Upgrade video/projection at ELC</li> </ul>	\$300,000
Fall of 2024	<ul style="list-style-type: none"> <li>Upgrade audio at CC, CN, CV, HL, and ELC</li> </ul>	\$225,000

While the physical classroom is important, likewise are the softwares provided by the district to support rigorous instruction, critical thinking, and student engagement. Like many districts, technology was quickly purchased to support remote learning during the height of the pandemic. As we begin to move through the pandemic, we know we need to reset and evaluate the software and digital instructional tools used in our classrooms.

DMTS purchased a software called CatchOn. In order to make determinations on software purchases, we needed to conduct an initial audit. CatchOn is a data analytics tool that allows the district to evaluate usage and efficiency of technology integrations and migrations. In conjunction with vendor analytics tools, and in partnership with Teaching and Learning, we have started the process of auditing our software applications, both licensed and non-licensed.

• **Screenshot of CatchOn Data**





Aligned to providing high-quality instructional tools, we must also ensure each tool is up to standards regarding student data privacy. The CatchOn platform also provides an easy way to monitor vendor privacy policies. This resource alerts the district when privacy policies have changed. Our team can quickly review the platform and make note of those changes. We are able to address issues in privacy policies that may cause us to stop using a particular tool or reallocate our grade level usage.

- **Screenshot of CatchOn's privacy policy tool**

Privacy policy updates

Date generated

05/09/2022

Compared versions

05/02/2022 and 05/09/2022

Privacy policies updated

2

Applications



Search

Privacy policy status

Search app by name

Q

Show all

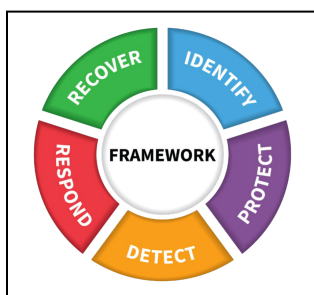
Application ^	Privacy policy status ^	App website	Privacy policy	Actions
 Code.org	Updated	<a href="#">View</a>	<a href="#">View</a>	<a href="#">View updates</a>
 Creative Cloud by Adobe	No changes	<a href="#">View</a>	<a href="#">View</a>	-

## Cybersecurity Landscape

Technology landscapes are evolving at a rapid pace. New technology is created and implemented every day. As such, cyber criminals are becoming ever more creative and adept at infiltrating systems. Schools hold an exorbitant amount of student and staff data. In addition, we know that human error is the number one greatest cause of cyber breaches. In conjunction with changing insurance requirements, and based on our philosophical belief in maintaining a robust security posture, we have and continue to make changes to our cybersecurity landscape.

DMTS has established a work group that focuses solely on cybersecurity. This group stays up-to-date on our current security posture, maintains cyber insurance requirements, and continues to explore ways we might stay ahead of cyber criminals.

We are in the early stages for the adoption of a cybersecurity framework to help guide and direct our work over the coming years. One such framework is the National Institute of Standards and Technology (NIST) framework. Adopting a framework across the district will impact our policies and procedures not only at DMTS, but also districtwide. It will allow us to make effective and efficient decisions around our daily practices, and cyber incidents.



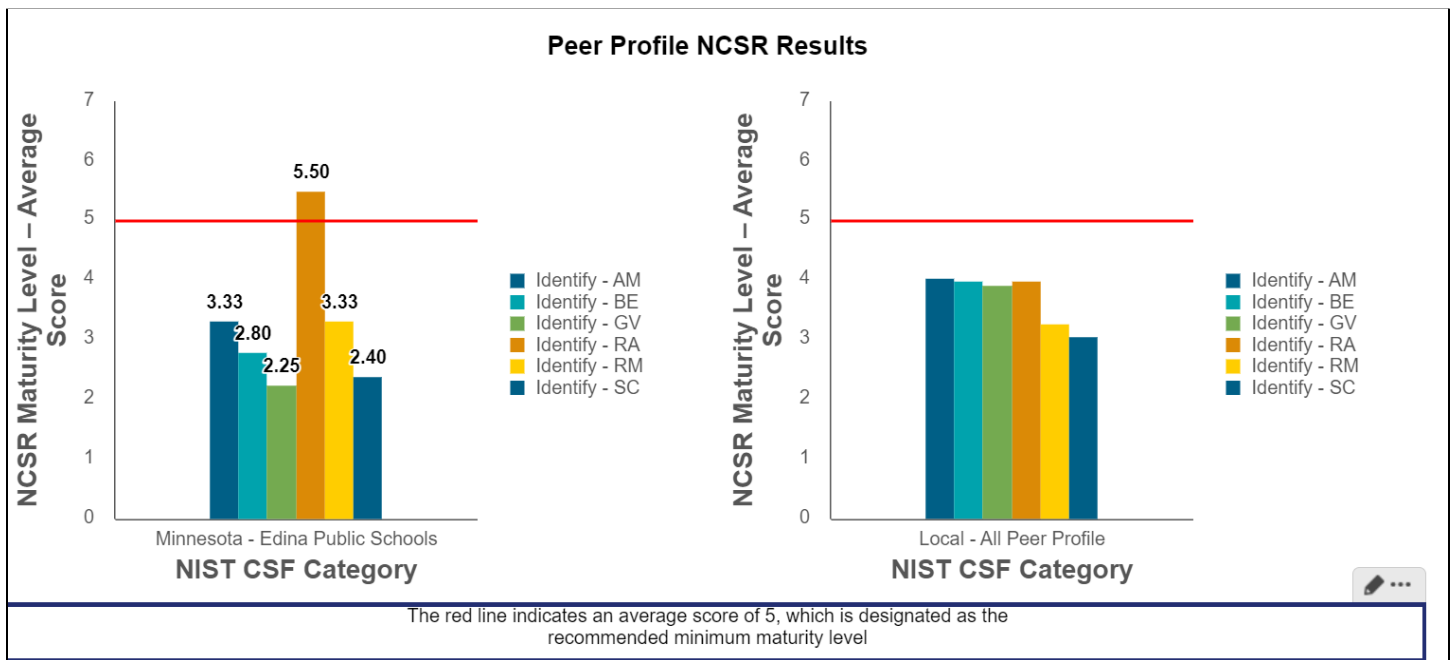
- **NIST Framework:** Cybersecurity framework with five key functions - identify, protect, detect, respond, recover.
  - Identify: Develop an organizational understanding to manage cybersecurity risk to: systems, assets, data, and capabilities



- Protect: Develop and implement the appropriate safeguards to ensure delivery of services
- Detect: Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event
- Respond: Develop and implement the appropriate activities to take action regarding a detected cybersecurity event
- Recover: Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event

(<https://www.nist.gov/cyberframework>, June 2022)

This year, our team completed the Nationwide Cybersecurity Review (NCSR). It is an annual self-assessment that allows our team to evaluate gaps and capabilities within our system. The feedback from the report also allows us to compare our security posture against like-organizations. Our team is currently working to develop benchmarks and metrics based on the 2021-22 NCSR results. This yearly trend data will also provide us insight with how we are improving our work.



The changing cyber landscape requires the district to meet several insurance requirements. All school districts are bound to cyber insurance policies. Based on our organization's size and financial posture, here is the list of the insurance requirements we have met or are working towards.

- MFA (multi-factor authentication) for all employee email access: Completed December 2021.
- MFA for all remote access to the network: Completed December 2021.
- MFA for all privileged user accounts: Ongoing.
- Offline backups or cloud backups: Implementation summer 2022.
- Endpoint detection and response (EDR) deployed across all endpoints: Implementation July 1, 2022.
- Network monitoring solution: Currently implemented, but ongoing evaluation.
- Annual phishing training and simulated attacks for all employees: System purchased and will be implemented fall of 2022.
- Email filtering software to filter all inbound and outbound messages for spam and malicious content: Currently a part of our environment.
- Patch management procedures: Ongoing.



This year we joined the Multi-State Information Sharing and Analysis Center (MS-ISAC ) through the Center for Internet Security Agency (CISA). MS-ISAC is a key resource for “cyber threat prevention, protection, response, and recovery (<https://www.cisecurity.org/ms-isac>, May 31, 2022).” Through this network we are provided with real-monitoring of systems, security experts, training, intelligence, and resources. The vast majority of this program’s resources are free. While this is our first year joining the group, the information gleaned has become invaluable. Over the next years, we will continue to dive into this resource and its capabilities.

Student data privacy remains an important topic amongst law makers and technology staff. Recently, Minnesota legislature passed [HF 2353](#). This law aims to protect student’s personal data primarily from technology vendors. The final bill highlights the following points:

- The majority of the requirements for data privacy and security fall to technology vendors.
- Districts are responsible for providing notice of digital tools (curriculum, testing, assessment) 30 days prior to the start of the school year. This notice will need to occur annually.
- Districts have 72 hours to notify families if a student’s device was accessed to “respond to an imminent threat to life or safety.”

The passage of this bill will cause us to evaluate some of our practices and procedures, but we are already doing many of the items required in this bill. Data privacy and security will remain a top priority for DMTS.

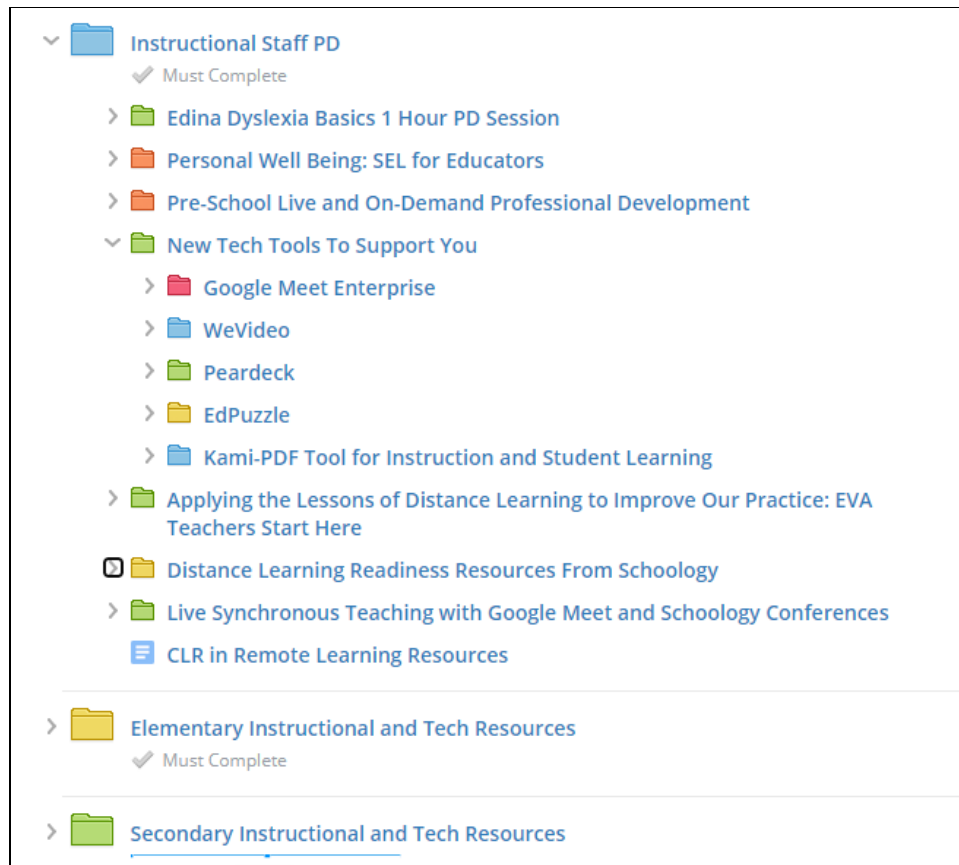
## **Technology Skills**

An important component of our work is to ensure all students have the requisite technology skills for all future endeavors. For this, we rely heavily on our media specialists (and classroom teachers). All K-12 media specialists are [CommonSense Certified Educators](#). A significant component to this certification is around student data privacy and digital citizenship. These skills are critical and foundational to a student’s future technology use.

To hone our student’s technology skills, it is critical that our staff have the necessary technology skills. The Digital Learning Specialists have offered ongoing professional development to support the growth of staff technology skills. The Digital Learning Coordinator will continue to provide staff with ongoing professional development, but we will also continue to offer asynchronous professional development options. In addition, we rely on our technology building paraprofessionals to provide support and media specialists to provide staff with a variety of technology skills that can be used in their roles.

- **Sample Staff PD Course**





## Where we are Headed

The pandemic shifted much of the way we do business, but in technology that is par for the course. Technology is an ever-changing landscape. - One that our team needs to stay on top of. Based on our work this year, we have several areas of focus moving forward.

- Continual development of an updated technology plan. As previously mentioned in this report, our work this year was the initial step of creating a long-range plan.
- Increased cybersecurity posture. Cybersecurity will be our major area of focus in the coming years. We will continue to work to ensure staff and student data is secure on our network. Likewise, we will need to do more to educate students, staff, and families on the importance of strong cybersecurity practices. Frankly, cybersecurity is a human issue. We can have all the systems put in place, but people need to understand the impact their choices may make on those systems. Education is key to that. We will also evaluate our human resources to see where we may allocate more dedicated service in the area of cybersecurity.
- Scope and sequence for student technology skills, based on the ISTE standards for students. We will work closely with our media specialists, Digital Learning Coordinator, Teaching & Learning departments, administrators, instructional leaders, and classroom teachers to ensure all students have future ready competencies pertaining to technology.



# Technology Report

2021-2022

June 13, 2022 School Board Meeting





# The Team



Brief Snapshot of our Service Environment	
Community	Total
Staff	~ 1975
Students	~ 8400
Technology	Quantity
Staff devices (laptops or desktops)	1,428
Student Chromebooks	6,410
Student iPads	2,421
Servers	94
Phones	1100
Wireless Access Points	550
Projectors	250
Interactive Whiteboards	230
Classroom Audio	300
Approved Student Tools	~ 170



# Digital Classroom Standards & Instruction

- Devices
  - K-1: 1:1 ipads
  - 2-8: 1:1 district Chromebooks
  - 9-12: Hybrid BYOD
- 3-year Digital Classroom Standards update
  - Audio Solution
  - Classroom projection
- CatchOn Data
  - Data
  - Privacy Policy





# Cybersecurity Landscape

- NIST Framework
  - Identify
  - Protect
  - Detect
  - Respond
  - Recover
- NCSR (Nationwide Cybersecurity Review)
- Cyber Insurance Requirements
- MS-ISAC (Multi-State Information Sharing & Analysis Center)
- HF 2353





# Technology Skills

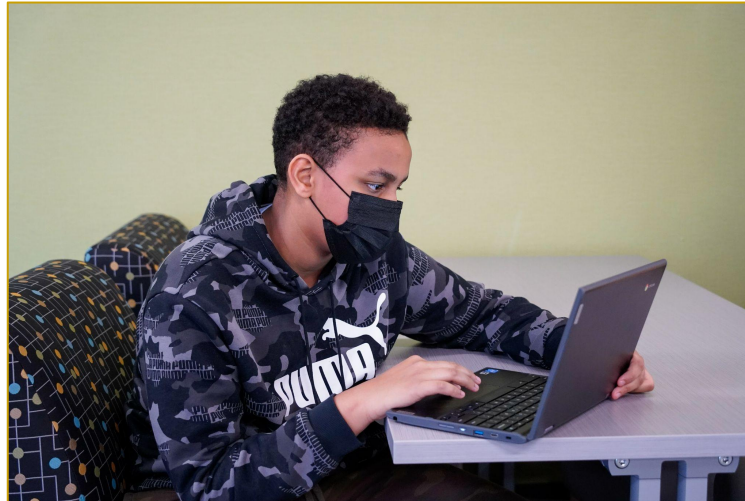
- CommonSense Certification at all buildings
- Professional Development offerings
- Continued emphasis and development on a scope and sequence





# Where we are headed

- Continual development of an updated technology plan
- Increased cybersecurity posture
- Scope and sequence for technology skills
- Whatever else comes our way!







**Board Meeting Date:** 6/13/22

**TITLE:** Board Officer Approval

**TYPE:** Action

**PRESENTER(S):** Board Chair Erica Allenburg

**BACKGROUND:** Due to moving out of the state, Vice Chair Leny Wallen-Friedman is no longer on the board as of May 31. This has left the position of Vice Chair vacant and needs to be filled. In filling the position of Vice Chair, other board roles could need to be filled as well.

**RECOMMENDATION:** Chair Allenburg will have a recommendation for the board to fill the positions at the meeting.

**PRIMARY ISSUE(S) TO CONSIDER:** The plan to fill board leadership roles.

**ATTACHMENTS:**

1. None.





**Board Meeting Date:** 06/13/2022

**TITLE:** Endpoint Detection and Response RFP Proposal Acceptance - Carbon Black

**TYPE:** Action

**PRESENTER(S):** Natasha Monsaas-Daly, Director, District Media & Technology Services

**BACKGROUND:** Edina Public Schools has a cyber risk policy through the District's insurance carrier. As a district with a revenue of 100m+, we are required to have EDR (endpoint detection and response) deployed across all of our device endpoints. We were notified of this requirement in April 2022. The due date to meet this requirement is July 1, 2022. Should we not meet this requirement, we will be at risk of not being covered by insurance in the event of a data breach. Additionally, having EDR is best practice in any organization.

EDR is a cybersecurity measure that provides monitoring and collection of endpoint data that may indicate a threat or threat patterns. This is a crucial piece of our cybersecurity posture. As threats increase, Edina Public Schools will need to continue to update and maintain our security stance. We are committed to ensuring that staff and student data and systems are safe and secure.

**RECOMMENDATION:** Consent to move forward with the purchase of Carbon Black EDR solution.

**PRIMARY ISSUE(S) TO CONSIDER:** Quote from CDW

**ATTACHMENTS:**

1. Quote (next page)



# Edina Public Schools

## Endpoint Detection and Response Protection

5/27/2022



## Education

© CDW Government LLC 2022 | 230 N. Milwaukee Ave. | Vernon Hills, IL 60061

To the extent allowable, all information and documents hereby submitted in response to the Request for Proposal ("RFP") furnished by Edina Public Schools are the Proprietary and Confidential property of CDW Government LLC ("CDW•G").



5/27/2022

Edina Public Schools  
5701 Normandale Rd  
Edina, MN, 55424



One CDW Way  
230 N. Milwaukee Avenue  
Vernon Hills, IL 60061  
P: 847.371.5800  
F: 847.465.6800  
Toll-free: 800.808.4239  
cdwg.com/PeopleWhoGetIT

RE: CDW Education Response to Edina Public Schools's Endpoint Detection and Response Protection RFP

Dear Kyle Trites,

CDW Education understands the objective of the RFP is for Edina Public Schools to identify a reliable and experienced supplier partner capable of managing your Endpoint Detection and Response Protection Solution. Our response demonstrates CDW Education's ability to contribute to the overall success of this initiative.

CDW Education is a specialized segment of CDW Government LLC ("CDW•G"), the wholly-owned subsidiary of CDW LLC. As a global systems integrator impacting 75 million students across 34 countries, we enable and empower over 17,000 education institutions to get the most out of the transformational impact of our partners' technology. Specific advantages of partnering with us include:

- Redundancy and Speed. Store products in one of our two US CDW-owned, ISO 9001:2015-certified distribution facilities. CDW can assist with equipment schedules and logistics.
- Turnkey with Breadth of Solutions. We are technology neutral with 100,000+ products and services from 1,000+ leading and emerging brands. We continually update these partners and products, allowing you access to industry-leading solutions.
- Dedicated Support. Highly trained and experienced account team, including a dedicated account manager is responsible for coordinating all of your needs and ensuring customer satisfaction.
- Financial Strength. Our financial stability stems from our vendor-neutral solutions and multiple dedicated customer channels. Multiple avenues for growth and a balanced customer base allow us to weather economic and technology cycles.

As always, we consistently strive to exceed your expectations. Should you have any questions regarding our response, please contact your account manager, Mayank Srivastava, at (312) 705-9366, or via email at mayasri@cdw.com. We thank you for the opportunity to participate in this RFP process and are confident you will find our response advantageous from both a strategic and budgetary standpoint.

Sincerely,

A handwritten signature in blue ink that reads "Justin Schwier". To the right of the signature are two asterisks (\*\*).

Justin Schwier  
Supervisor, Proposals  
CDW Education

\*\*See attached CDWG Terms of Offer found on page 19 of this response submission.



# Company Overview

CDW Education understands that the objective of this RFx is for Edina Public Schools to identify the most reliable and experienced provider for Endpoint Detection and Response Protection. Whatever the driving force behind your technology needs, we can support you where you are and help you achieve your goals—present and future—with the right solutions, precisely implemented, which can evolve with your organization.

Along with unwavering customer focus, we are committed to technology solutions delivering the best possible service and support with one-stop shopping for customized solutions. No matter where you are on your technology journey, Edina Public Schools gets more from your IT investment through our Technology Services, from roadmaps and adoption to project deployment and lifecycle management. Some benefits Edina Public Schools will realize when partnering with CDW Education are:

- Accessibility, reliability, and consistency for a smoother experience
- Greater efficiencies through automated operations, agility, and scalability
- Increased infrastructure security with preventative and proactive protection and remediation
- Robust solution development for your unique challenges by experienced and knowledgeable engineers.
- Integrated technology solutions designed, implemented, and managed by highly specialized solution architects who can help you capitalize on new opportunities
- Management of your technology environment today and into the future with lifecycle technical and customer support, from presales consultations to post-implementation issue resolution
- Savings of time money by supplementing your IT staff quickly with award-winning staff augmentation
- A strong partnership with individuals Edina Public Schools knows and trusts due to high retention of quality coworkers motivated to maximize performance and productivity.

## ABOUT CDW EDUCATION

CDW Education is a specialized segment of CDW Government LLC (“CDW•G”), the wholly-owned subsidiary of CDW LLC, a leading multi-brand technology solutions provider to business, government, education and healthcare organizations in the United States, the United Kingdom and Canada. Recognizing the unique challenges and opportunities of our public sector customers, we established CDW•G in 1998 to focus on the specific needs of the government and education sectors. Our teams are broken down by segment, with

### CDW Quick Facts

**Vernon Hills, IL**  
Headquarters

**\$21B**  
2021 Annual Net Sales

**14,000**  
Coworkers

**28**  
U.S. Sales Offices

**250,000+**  
Customers

**161**  
2021 Fortune 500 Rank



separate teams serving State and Local customers, K-12, Higher Education, and Federal, and further organized into 11 geographic regions for a higher level of specialization. Our customer base is quite diverse, ranging from state and local government, federal, healthcare, K-12 and higher education. We have an expansive network of offices near major cities and a large team of field coworkers across the United States. As a global systems integrator impacting 75 million students across 34 countries, CDW Education enables and empowers over 17,000 education institutions to get the most out of the transformational impact of our partners' technology.

CDW debuted on the Fortune 500 in 2001. and now ranks at number 161. CDW ranks at No. 5 on CRN's 2021 Solution Provider 500 list. The sustainable growth and continued financial stability of our company serves to assure Edina Public Schools that we are here to stay and can support you through the life of this contract and beyond.

## **WE GET Classroom IT**

You will find that CDW Education addresses Edina Public Schools' RFP requirements to highlight our proposed value-added services; aimed at increasing educator effectiveness, saving you budget dollars and saving you valuable IT staff time. We hope to bring forth the kinds of solutions that will make for more smiles and success among parents, teachers, students, and staff.

### **We are a trusted technology partner to more than 15,000 K-12 schools.**

We have experience handling complex deployments for the largest school districts in the country. We have deployed devices nationwide, and we have the logistics capabilities to get your devices to your students, even in adverse conditions. Over the past 20+ years, CDW's technology infrastructure solutions have stayed in line with emerging technologies. Keeping up with those technologies, such as collaboration solutions, cloud, mobility and virtualization, has been a major aspect of our ability to grow as a company. In 2020, CDW acquired Amplified IT, a leading provider of education-focused services and cloud-based software, enabling and empowering schools to leverage the innovation of Google for Education and Google Cloud.

## **WE GET Empowering Your Classroom**


Empower your students, teachers, administrators and parents to explore and build opportunities for improving academic outcomes. From selecting the right mobile devices to ensuring seamless connectivity and accessibility, we can help you orchestrate highly effective personalized learning environments

Balancing the challenge of maximizing your students' digital freedom while simultaneously keeping them protected is no easy task. You must also ensure your teachers are supported with the digital autonomy they need to educate your students. Innovative uses of educational devices including Chromebooks and Windows 10 can help you overcome this challenge and achieve digital freedom and security. CDW Education can assist you with implementing content filtering and classroom management techniques, finding the right storage solutions and determining your new software workflow.



## WE GET Reliable Distribution

Unlike many solutions integrators, CDW operates physical warehouses as opposed to the virtual warehouse methodology. CDW has two large, strategically located distribution centers controlled by a state-of-the-art Warehouse Management System (WMS) that ensures speed and accuracy throughout the order fulfillment and distribution processes. CDW has a 450,000-square-foot distribution center located at our headquarters in Vernon Hills, IL and a 513,000-square-foot distribution center located in North Las Vegas, NV. These locations facilitate quick distribution of products to our growing customer base throughout the country. The Vernon Hills (VH) distribution center focuses on distributing products to customers east of the Mississippi River while the Las Vegas (LV) distribution center primarily serves the western part of the United States.



**LAS VEGAS, NV**  
513k square feet  
Capacity for up to 10K+ configurations per day



**VERNON HILLS, IL**  
450k square feet  
Capacity for up to 10K+ configurations per day

OUR CONFIGURATION CENTERS ARE PCI CERTIFIED AND HOLD SEVERAL ISO CERTIFICATIONS:

**ISO 9001**  
Quality

**ISO 14001**  
Environmental

**ISO 20243**  
Risk Management

**ISO 27001**  
Information Security

**ISO 28000**  
Secure Supply Chain

CDW holds more than \$300M of available inventory in our two CDW-owned distribution centers that total almost 1M square feet. Our ISO 9001, 14001 and 28000 certified strategically located distribution centers provide speed, accuracy, and excellent geographic coverage across the United States. We have access to more than 100,000 top brand-name products from more than 1,000 leading manufacturers.

## WE GET Secure Supply Chain

Inventory availability and reliable distribution are not the only key elements in effective purchasing. More and more, organizations rely on information and communication technology to handle growing workloads and mission-critical operations. In this increasingly uncertain world, they are facing a dangerous reality: the rise of counterfeit and maliciously tainted equipment. Customer can be confident in the quality of the products you order through CDW. ISO 28000:2007 Secure Supply Chain is an important standard for our company. The scope of the certification includes planning, deployment, and provisioning of supply chain services and supporting processes. ISO 28000:2007 certification demonstrates that CDW has mature, end-



to-end risk management programs, with a focus on delivering quality and security in managing information, products, and services to meet our customers' needs.

## WE GET Strong Manufacturer and Distribution Partnerships

A significant advantage we offer Edina Public Schools is our ability to deliver the right products, at the right value, right when you need them. As one of the largest direct market resellers, CDW has established exceptional working relationships with the major manufacturers in the technology industry. Our buying power attracts the industry's top manufacturers – and their best prices. To supplement our direct purchasing model, CDW has developed strong affiliations with principal channel distributors. Our distribution centers are located in close proximity to principal distributors; this enables us to quickly obtain competitively priced, non-stocked items.

Some of our strongest manufacturer and software publisher partnerships and designation levels are provided below.

CDW Partnerships	
Partner	Designation
Acer	CDW is largest B2B partner in the U.S.
Adobe	Largest Platinum partner in the US and Worldwide
Cisco	Largest U.S. Direct Reseller, Gold Certified Partner
Dell	#1 National Solution Provider Partner, Titanium Partner
HP Enterprise	#1 Global Channel Partner
HP Inc.	#1 Commercial Channel Partner, Platinum Partner
IBM	Platinum IBM Business Partner
Lenovo	#1 Global Partner
Microsoft	Gold Certified Partner
VMware	Largest Corporate Reseller Among the America's Channel Partner Organization



# Professional Services

CDW Services offer you an unusual combination: the close relationship and easy access of a local provider who understands your IT environment inside and out, and the scale, efficiency and resources of a multinational provider. CDW is ranked No. 5 on CRN's 2021 Solution Provider 500 list, a ranking of the largest IT solution providers in North America by revenue. Our deep expertise across a full range of integrated technology solutions backed by deep industry specialization allows us to provide flexible, end-to-end services to our customers. Our on-demand resources provide the assistance and scale your IT team needs — freeing them up to focus on delivering bottom-line value and innovation.

## Local Attention

CDW is headquartered just outside of Chicago, Ill., and we have 28-plus local branch offices throughout the United States and Canada. So, chances are, we're within driving distance of your office. And even if you're located in an area without a local CDW branch, our network of trusted service providers — all trained to follow the same consistent approach, processes, methodologies and professional manner of CDW-badged engineers — ensure that your organization will still get the full attention and resources it deserves.

## National Scale

For U.S. customers, our operational footprint is abundantly national, with offices located in every region and two state-of-the-art distribution centers strategically located for the fastest possible service. We have full redundancy, eProcurement integration and provider consolidation available to further increase our cost and service efficiencies. In addition to our local branches, we have over 1,100 services professionals and a fast-growing network of trusted service and solutions partners. In fact, because of our national scale, CDW is able to identify areas of emerging need for our customers and then ramp up our expertise and resourcing in those areas.

## Project Management

We understand that a well-defined project structure is important and key to the success of an engagement. CDW's Project Management Methodology provides a roadmap to the processes, roles, and checkpoints that govern work with our customers from proposal development through service delivery. CDW's Project Methodology offers flexibility and judgment, yet provides a clear path for the engagement to follow. We draw upon best practices derived from the IT Infrastructure Library (ITIL) framework. Our methodology enables us to support each customer engagement "The CDW Way." A dedicated CDW Project Manager will provide a single point of contact and escalation point to ensure the success of the entire project.

### CDW Amplified™ Services



Security



Infrastructure



Workspace



Support



Data



Development



# Value-Added Resources & Account Management Team

CDW offers an account management structure that focuses on providing value-added presales consulting and comprehensive support throughout the lifecycle management of your assets. When you work with CDW, you have access to expertise that is not available within your organization. Your CDW Account Management Team coordinates with the applicable value-added resources to help your organization develop the best solution for your specific needs, challenges, and long-term goals.

## Account Management Team

Your dedicated account management team is responsible for managing your procurement needs and overseeing all facets of your account. Key personnel include:

### Mayank Srivastava, Executive Account Manager

P: (312) 705-9366, E: mayasri@cdw.com

Mayank Srivastava serves as Edina Public Schools' primary point of contact. Mayank is available on an as-needed basis to tackle all of Edina Public Schools' product quote, order placement, and problem resolution needs. With over 14 years of CDW tenure, Mayank Srivastava is highly trained to address your questions and concerns. Having managed numerous accounts based in the Edina region, Mayank is extremely familiar with the processes, challenges, and needs that are specific to organizations similar to Edina Public Schools.

### Valerie Hanrahan, Sales Manager

P: (312) 547-2711, E: valeban@cdw.com

Valerie Hanrahan oversees your account team and helps to develop strategies that best serve your organization's long-term success. Valerie spends a significant amount of time meeting with customers to understand the dynamics of their local markets and to ensure that they take full advantage of CDW's offerings. Also, she is responsible for building and maintaining strong relationships locally with our top OEM partners. Valerie's ability to leverage those relationships will greatly benefit your organization. Valerie Hanrahan has been employed at CDW since 2014.

## Presales Consulting Expertise

A unique advantage of CDW's business model is that Edina Public Schools has access to an incomparable depth and breadth of value-added technical expertise. Your CDW Account Team includes highly trained presales specialists who are experts in particular areas of technology or for specific partner products. These resources include Technology Specialists, Presales Systems Engineers, Solution Architects, and Onsite Vendor Representatives.



Your account manager engages these value-added resources to bring Edina Public Schools the best advice and technology solutions to meet your unique needs. Your account team coordinates meetings Edina Public Schools and vendors to review future needs, standards, and roadmaps. In addition, your account team has access to dedicated manufacturer representatives who are onsite at CDW's sales offices to provide guidance and support.

## Ongoing Customer Support

CDW strives to provide outstanding customer support and resolve issues quickly so your organization will maintain a high level of productivity. While your account manager can generally handle most issues and concerns, our Technical Support, Customer Relations, and Site Support staffs are available to help. CDW•G has customer relations representatives who are available to resolve post-sales inquiries from 7:00 a.m. until 9:00 p.m. CT, Monday through Friday. We service customers through phone support, email, and live chat.

Excellence in customer service is a top priority for CDW•G. We have many quality controls and metrics in place to ensure high quality standards across the organization. We track and monitor a variety of service metrics and ratios daily to ensure that we provide continuous, high-quality customer service. We make adjustments and evaluate process changes as needed when we see high volumes for particular types of issues.





## REQUEST FOR PROPOSAL:

### MSSP/EDR SOLUTIONS

#### Opportunity Overview

ISD #273 – Edina Public Schools ("DISTRICT") is currently accepting proposals from qualified service providers ("Vendor") to implement and support an Endpoint Detection and Response Protection for Edina Public Schools Systems. This RFP is designed to provide interested parties with sufficient information to submit qualified proposals in which the district can select the best fitting vendor.

The Information Technology Services Department intends to implement the procured solution on 7/1/2022 to meet the requirements of the District's cyber security insurance policy.

#### Contract Terms

The contract would be for annual terms, renewable up to four years (total).

#### Proposals Submission Process

1. Review the Terms and Conditions to confirm eligibility
2. Complete pricing worksheet provided
3. Review all data, specifications, and requirements found in this document.
4. Questions can be submitted via email to [ktrites@catalyst sourcing.com](mailto:ktrites@catalyst sourcing.com) (or by contacting Kyle Trites at 612-669-6445)
  - *The District will not be responsible for, nor honor any claims resulting from, or alleged to be the result of misunderstanding by the vendor. It is the vendor's responsibility to bring all discrepancies, ambiguities, omissions, or matters that need clarification to the District's attention.*
5. Submission of proposals
  - **Proposals will be due on 5/27/2022 at 11:00 AM (CST)**
    - Proposals can be submitted via email to [ktrites@catalyst sourcing.com](mailto:ktrites@catalyst sourcing.com)
  - **All proposals submitted should include:**
    - Completed proposal worksheet (provided in this document)
    - Information about your organization, solution, and capabilities
    - Draft of your:
      - Scope of services/subscription agreement
      - Implementation/training plan

#### Process Timeline

Item Description	Date
<i>Request for Proposal (RFP) Documentation Released</i>	<b>5/17/2022</b>
<i>Deadline to Submit Questions</i>	<b>5/20/2022</b>
<i>Proposals/Quotes Due</i>	<b>5/27/2022</b>
<i>Selection</i>	<b>6/13/2022</b>



## Terms and Conditions

- A. Eligibility & Compliance with Federal and State Law - RFP must assure District that they have complied with all applicable Federal and State laws, regulations and rules.
- B. Invitation: The invitation for an RFP, which is attached hereto, and everything contained therein is adopted by reference and made part of these specifications and conditions.
- C. Agreement duration: The agreement will be for the period of three years from signature date. An additional one-year renewal term can be exercised by the district.
- D. General Criteria for Award: After taking into consideration conformity with the specifications, terms of delivery and other conditions imposed in the call for proposals, an award shall be made to the lowest responsible vendor.
- E. Writing: Within ten days of the award, persons having authority to contract for the parties shall duly execute a formal contract covering the subject matter of the RFP.
- F. Form of Proposals: The proposal must be submitted on the form prescribed by the District, a worksheet of which is contained in these specifications, and copies of which are available from the school District.
- G. Vendor's Qualifications: The District reserves the right to refuse to consider the proposal of a vendor who is not known to be reliable, skilled, and regularly engaged in providing the service and goods for which the vendors were invited. In addition, the District may require of any vendor evidence satisfactory to the District, of the vendor's financial responsibility, and ability to efficiently, economically and satisfactorily perform the services and deliver the goods required by the District. The District may consider the foregoing factors in determining the lowest responsible vendors.
- H. Rejection of Proposals: In addition to grounds for rejection stated elsewhere in law, or in these specifications and conditions, the District may reject an RFP if:
  - 1) The vendor fails to provide reasonable evidence reasonably requested pursuant to G.
  - 2) The vendor misstates or conceals any material fact in the RFP, **OR**
  - 3) The proposal is conditional. Proposals properly made subject to an escalator clause shall not be deemed conditional.
- I. Identical/Equal Proposals: In the case of identical proposals from two or more vendors, the board may at its discretion utilize negotiated procurement methods with the tied low proposals for that particular transaction, so long as the price paid does not exceed the original quote.
- J. Single RFP: In the case where only a single RFP is received, the board may, at its discretion, negotiate a mutually agreeable contract with the providing vendor so long as the price paid does not exceed the original quote.
- K. Withdrawal and Award Deadlines: No proposals may withdraw his/her RFP within 30 days after the date of opening of proposals. The District may elect to take up to 60 days to decide which proposals is to receive the award.
- L. RFP and Award Options: School District #273 reserves the right to
  - 1) Award this contract in part or whole to a single vendor
  - 2) Reject any or all proposals
  - 3) Award contract based on the investigation of a vendor, as well as acceptance of alternates, including the bond alternate, all of which the Owner deems to be in his best interest
  - 4) Waive informalities or minor irregularities in proposals and waive minor irregularities or discrepancies in RFP procedure
  - 5) Cancel a contract entered into with the successful vendor at any time, upon 30 days' written notice, to the contract vendor if the District's standards are not met
  - 6) the District is solely responsible for rendering the decision in matters of interpretation of all terms and conditions.
  - 7) The Owner, in determining the lowest responsible vendor, will consider in addition to the RFP process, the quality, suitability and adaptability of the item(s) to be purchased for the use for which it is intended.
  - 8) Trade-in policy and allowances will be considered where appropriate.
- M. Collusion: Conspiracy between vendors is cause for rejection of all proposals of vendors thus involved.
- N. Insurance Requirements: You will be required to provide proof of insurance as requested by District. Coverage levels described below should be considered MINIMUM requirements.

Insurance	Description	Coverage	Aggregate
Worker's Compensation	State Statutory Employer's Liability	\$500,000	n/a
Comprehensive General Liability (including Premises-Operations; Independent Contractor's Protective; Products and Completed Operations; Broad-Form Property Damage)	Bodily Injury; Property Damage; Combined Single Limit	\$1,000,000 each occurrence	\$2,000,000 aggregate
Blanket Contractual Liability	Bodily Injury; Property Damage; Combined Single Limit	\$1,000,000 each occurrence	\$2,000,000 aggregate
	Personal Injury, with Employment Exclusion Deleted	\$1,000,000 each occurrence	\$2,000,000 aggregate
Comprehensive Automobile Liability	Bodily Injury; Property Damage; Combined Single Limit	\$1,000,000 each occurrence	\$2,000,000 aggregate

- O. Guarantee: The successful vendor shall agree to unconditionally guarantee all goods supplied against inferiority as to specifications and conditions. All products delivered to the District shall be packaged under applicable federal, state and local requirements. Any items, which are rejected by the District because of damage, defect, or spoilage shall be removed and replaced without cost to the District.
- P. Non-Waiver of Specifications and Conditions: Failure or neglect of the District to require compliance with any term, condition, or specification of the RFP shall not be deemed a waiver of the same.
- Q. Terms of Payment: Payments will be according to Minnesota Statute 471.425, currently providing for payment within 35 days after receipt of the merchandise or the invoice, whichever comes latest. Nothing in the vendor's, contract, or invoice will override this provision



## Current Environment

### Servers that can take an EDR installation

Server Locations	Physical Machine	Virtual Machine	Internal	Public
Edina Community Center	8	60	63	5 (all VMs)
Edina High School	1	2	3	0
Microsoft Azure Cloud	0	2	1	1

### End Points (minimum)

	# Workstations
Domain-Joined Windows and Linux Workstations	1,500

## Preferred Functional Capabilities

- Must be able to prevent District systems from Zero-Day exploits & attacks.
- Solution must not rely SOLELY on signature-based detection and protection methods.
- The solution must identify malicious files and prevent them from execution, including viruses, trojans, ransomware, spyware, crypto miners and block usage of common attack tools.
- The solution must identify malicious behavior of executed files, running processes, registry modifications, or memory access and terminate them at runtime, or raise an alert.
- Solution should have a proven track record on effectively preventing enterprise endpoint systems from Ransomware and other types of advanced threats.
- Must be able to interoperate with future SIEM, IDS/IPS and other information security systems to provide additional level of protection through early threat detection and prevention.
- Must be able to provide protection for diverse District digital assets including laptops, servers and workstations.
- Provide a consistent, functional, centralized administrative interface that is intuitive and easy to navigate.
- The solution should be able to automate the endpoint prevention by autonomously reprogramming and retuning itself using threat intelligence gained from behavioral analysis, reputation, and machine learning.
- The solution's agent should have a minimum footprint and performance impact on the District endpoints (should not noticeably impact end user's computing experience during scanning or continuous protection).
  - Doesn't rely on resource intensive detection and protection methods that can adversely affect the performance of installed District devices.
- Must provide automated alert notification (email, text, etc.) to District staff regarding suspicious activities that may pose security threat to the District's assets.
- Solution must uniformly automate information security operational workloads across the District's diverse operating environment.
- The cloud based administrative console should be scalable to accommodate all related District workloads and must be resilient enough to provide maximum uptime.
- The vendor should provide 24x7 product support over multiple channels.
- The vendor is expected to provide timely support for project planning, deployment, problem resolution to assure a 7/1/2022 launch.
- The vendor is expected to perform knowledge transfer of all necessary operational matter to District staff to ensure effective future management and maintenance of all ongoing operations.
- The EDR solution should be managed by live staff in a 24x7 SOC who have the ability to disable or network isolate a system that is infected if it cannot be fully or confidently mitigated, as well as working to prevent lateral movement of the infection. No interaction from District staff should be needed to mitigate or network isolate infected systems that are considered highly infectious or detrimental to other systems or ongoing operations for the District network.

## Implementation Specifications

Vendor must provide best industry practices for the implementation and management of proposed systems. The selected vendor must provide knowledge transfer of all relevant information.

### Testing, Staging and Deployment Schedule

- Vendors are required to submit the complete project plan and action steps clearly specifying execution items.
- The vendor is required to provide product road map (coming features) and its associated delivery date.
- The vendor must provide a summary of known outstanding issues with the current version of the proposed solution and expected resolutions.
- Vendors must work in such a manner that school district business is not affected in any way.
- Configure the management console to provide required functionality outlined in this RFP.
- Describe any monitoring tools or plug-ins (i.e. product console plug-ins) that is available to monitor the system.

### Training and Support

- Provide training for up to six (6) District employees to configure, operate, and maintain your proposed solution.
- Formal training can be remote but must cover all key concepts and be specific to the proposed solution.



## RFP Worksheet

### Your Company Information

Company Name	CDW Government LLC	Contact Name	Mayank Srivastava
Address	230 N Milwaukee Ave	City	Vernon Hills
State	Illinois	Zip	60061
Phone	(312) 705-9366	Email	mayasri@cdw.com

### References\*

Organization	Contact Name	Contact Email
<p>VMware is proud to count some of the most trusted organizations in the world among our customers. We have many customers who have offered to be public references, which can be viewed on our Customer Stories page at <a href="https://www.vmware.com/company/customers/index.html#">https://www.vmware.com/company/customers/index.html#</a></p> <p>VMware can provide specific customer contact details as we move through your evaluation process.</p>		

\*School districts preferred

### General/Confirmation Questions

Question	Your response
Have you reviewed and accept the terms and conditions outlined in this document? <b>[Y/N]</b>	Y
Are you eligible to do business with public school districts in the State of Minnesota? <b>[Y/N]</b>	Y
Have you included a draft of your standard scope/subscription agreement? <b>[Y/N]</b>	Y
Can your solution meet the standard cyber insurance endpoint detection and response requirements? <b>[Y/N]</b>	Y

### Solution Performance & Capability Data Points

Data Point	Your response
Does your solution function at the <b>Endpoint-level</b> or is it <b>Agent</b> based?	Our solution is cloud based, but every endpoint would have a light weight agent deployed to it.
Provide a high-level methodology of how your solution detects and responds to threats.	VMware Carbon Black provides a layered approach of detective and preventative capabilities fueled by a continuous process activity monitoring system. Signature-based detection, pattern recognition of malware variants, and contextual analysis of process behavioral patterns ensure protection regardless of threat category (spyware, adware, trojan, etc.)
How does your solution communicate threats and status to District managers?	Administrators of the VMware Carbon Black Cloud platform can create notification preferences to ensure timely email communication of threat activity to relevant personnel.



Are there any known conflicts with other antivirus products, specifically Windows Defender?	Adding mutual exclusions in endpoint protection platforms is always a recommended practice when installing alongside a pre-existing solution. That said, there are no known conflicts between the VMware Carbon Black Cloud agent and Windows Defender. Upon installation, Windows Defender will autonomously relinquish its antivirus duties and VMware Carbon Black will show as the antivirus in Windows Security Center.
Are there known conflicts with other endpoint solutions?	There are no known conflicts but adding mutual exclusions in co-resident endpoint protection platforms is always a recommended best practice to avoid novel race conditions.

### Solution Performance & Capability Data Points (cont'd)

Data Point	Your response
Please describe how data is reported and accessible by the District staff.	Data is gathered locally on each endpoint by the VMware Carbon Black Cloud agent. Each agent communicated back to your organizations tenant a record of event logs and/or alert activity every few minutes. These alert and events are maintained and available to the appropriate District staff per your environment's role-based access control settings. You can also generate pdf or csv reports of dashboard information that is collected.
Are tools provided to explore current and historical threat data collected by the solution?	The Carbon Black Cloud provides 30 days of retention out of the box for all data and 180 days for alert data. Searching within the platform does not require mastery of complex querying languages and will provide market-leading yet accessible visibility.
Where is reporting data stored?	In an organizations independent tenant on the VMware Carbon Black Cloud platform, hosted on AWS NA
What is your solution's false positive rate?	Each customer's instance is unique and there numerous factors that could contribute to this calculation. With that said, third parties have provided insight on the favorable efficacy of the VMware Carbon Black cloud. Reference: <a href="https://www.vmware.com/security/product-certifications-and-public-testing.html">https://www.vmware.com/security/product-certifications-and-public-testing.html</a> and <a href="https://attacker.mitre-engenuity.org/enterprise/participants/vmware/?adversary=carbanak_fin7">https://attacker.mitre-engenuity.org/enterprise/participants/vmware/?adversary=carbanak_fin7</a>
What is your solution's false negative rate?	Each customer's instance is unique and there numerous factors that could contribute to this calculation. With that said, third parties have provided insight on the favorable efficacy of the VMware Carbon Black cloud. Reference: <a href="https://www.vmware.com/security/product-certifications-and-public-testing.html">https://www.vmware.com/security/product-certifications-and-public-testing.html</a> and <a href="https://attacker.mitre-engenuity.org/enterprise/participants/vmware/?adversary=carbanak_fin7">https://attacker.mitre-engenuity.org/enterprise/participants/vmware/?adversary=carbanak_fin7</a>
How much CPU and Memory does the solution use?	<1% CPU, Memory (RAM) = 150-200MB on average (no spikes as is commonly observed with traditional AV)  <a href="https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/cbc-endpoint-standard-oer/GUID-A41CFFE1-AC5B-497F-B4B7-EFEF0979332B.html">https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/cbc-endpoint-standard-oer/GUID-A41CFFE1-AC5B-497F-B4B7-EFEF0979332B.html</a>
Does your solution have the capabilities to automatically update both definitions and software version without user involvement?	Definition update automatically on a default cadence of once every four hours that is configurable. Sensor versions can be easily updated from the administrative platform, or optionally through software management tools if desired.

### Projected Timeline

Question/Data Point	Response
How much time is required to implement your solution following the signing of the agreement?	<p>Following the signing of an agreement, a tenant will be created for the District in the VMware Carbon Black Cloud and delivered, marking license fulfillment. Once delivered, the District may proceed with implementation at whatever rate they are prepared to deploy agents across the environment.</p> <p>Additionally, Professional Services are available for assistance throughout an implementation project. An implementation project begins with a team of Carbon Black implementation specialists assisting your team in planning and deploying Carbon Black products throughout your environment. Our team leverages</p>



	<p>established templates, tools, and best practices honed across thousands of deployments to efficiently guide your team during scheduled working sessions.</p> <p>Our consultants and engagement managers will work collaboratively with your team to review your IT security needs and to tune our solutions as needed to meet those needs. We provide packaged services offerings for each of our products to quickly and easily get started with the products as well as to optimize the use of the solutions overtime providing a full lifecycle of value for whichever Carbon Black products you chose.</p> <p>For details on our Quick Start Implementation packages, please visit <a href="https://www.carbonblack.com/license-agreements">https://www.carbonblack.com/license-agreements</a></p>
--	---

## Solution Cost

Data Point	Your response
How do you price your solution (per end point, per server, etc.)?	Per Endpoint Per Year
Is your proposed pricing GUARANTEED for the life of the agreement (4-years)? [Y/N]	District has option of purchasing 1, 3, or 5 years in advance. Annual renewal typically sees <5% increase

## Solution Cost based on current environment

Data Point	Your response
Proposed Annual Licensing and Support cost:	\$21.00 x 1500units
Proposed Hardware cost:	
Proposed implementation/installation/training cost:	\$2600.00
<b>FIRST YEAR TOTAL COST:</b>	<b>\$34,100.00</b>



# Pricing Offer



# QUOTE CONFIRMATION



DEAR NATASHA MONSAAS-DALY,

Thank you for considering CDW•G LLC for your computing needs. The details of your quote are below.  
[Click here](#) to convert your quote to an order.

QUOTE #	QUOTE DATE	QUOTE REFERENCE	CUSTOMER #	GRAND TOTAL
MSZL249	5/6/2022	CARBON BLACK + MDR FROM VMWARE	4079074	\$34,100.00

QUOTE DETAILS				
ITEM	QTY	CDW#	UNIT PRICE	EXT. PRICE
<a href="#">VMware Carbon Black Cloud Endpoint Standard - subscription license (1 year)</a> Mfg. Part#: VSEC-CBES-DIR-W-US-1Y-A Electronic distribution - NO MEDIA Contract: MARKET	1500	5959231	\$16.00	\$24,000.00
<a href="#">VMware Carbon Black Cloud Managed Detection and Response - subscription lic</a> Mfg. Part#: VSEC-MDR-DIR-US-1Y-A-PRO Electronic distribution - NO MEDIA Contract: MARKET	1500	6829430	\$5.00	\$7,500.00
<a href="#">VMware Carbon Black Cloud Deployment Essentials - installation configurat</a> Mfg. Part#: VSEC-CBC-PS-DP-ESSL Electronic distribution - NO MEDIA Contract: MARKET	1	6708327	\$2,600.00	\$2,600.00

PURCHASER BILLING INFO	SUBTOTAL	\$34,100.00
<b>Billing Address:</b> EDINA PUBLIC SCHOOLS - ISD 273 ACCOUNTS PAYABLE 5701 NORMANDALE RD EDINA, MN 55424-2401 <b>Phone:</b> (952) 848-3900 <b>Payment Terms:</b> NET 30-VERBAL	SHIPPING	\$0.00
	SALES TAX	\$0.00
	GRAND TOTAL	\$34,100.00
DELIVER TO	<b>Please remit payments to:</b>  CDW Government 75 Remittance Drive Suite 1515 Chicago, IL 60675-1515	
<b>Shipping Address:</b> EDINA PUBLIC SCHOOLS - ISD 273 EDINA PS 5701 NORMANDALE RD EDINA, MN 55424-2401 <b>Phone:</b> (952) 848-3900 <b>Shipping Method:</b> ELECTRONIC DISTRIBUTION		

Need Assistance? CDW•G LLC SALES CONTACT INFORMATION



Mayank Srivastava

(866) 626-8519

mayasri@cdw.com

This quote is subject to CDW's Terms and Conditions of Sales and Service Projects at



<http://www.cdwg.com/content/terms-conditions/product-sales.aspx>

For more information, contact a CDW account manager

© 2022 CDW•G LLC 200 N. Milwaukee Avenue, Vernon Hills, IL 60061 | 800.808.4239



# CDW•G Terms of Offer

To the extent allowable, all information and documents hereby submitted in response to the Request for Proposal (“RFP”) furnished by University of Southern Mississippi are the property of and are proprietary to CDW Government, LLC (“CDW•G”).

Notwithstanding anything to the contrary contained in the Proposal, CDW•G declares its understanding that CDW•G’s Terms and Conditions of Product Sales and Service Projects (“T&C”), as updated from time to time and provided on CDW•G’s website at <https://www.cdw.com/content/terms-conditions/product-sales.aspx> , constitute the terms and conditions controlling the transaction contemplated by the RFP, except as otherwise agreed upon in writing by the parties. CDW•G requests that Customer review and confirm acceptance of the T&C or, if necessary, negotiate with CDW a mutually agreeable final contract. CDW•G shall not be bound to any term(s) of the RFP or the Proposal or to any contract related to the RFP until or unless: (i) Customer confirms in writing its acceptance of the T&C; or (ii) authorized representatives of CDW•G and Customer execute a written contract that is separate from the Proposal.

Except as otherwise set forth above, CDW•G agrees to maintain the validity of the Proposal for a period of thirty (30) days from the RFP-established due date (“Validity Period”), provided that there are no extraordinary changes in pricing due to unique market conditions, product discontinuation, manufacturer price changes, or other extenuating circumstances. In order to ensure CDW•G’s commitment to the pricing levels and other proposed offerings contained in the Proposal, Customer may notify CDW•G via mail or e-mail that either: (i) Customer accepts CDW•G’s Proposal and agrees to be bound by the T&C, or (ii) Customer intends to negotiate with CDW•G a separate agreement during the Validity Period.

CDW•G will conduct any negotiation of a final agreement with Customer in good faith. Notwithstanding the foregoing, any prices or other privileges contemplated in the Proposal shall commence on the effective date of agreement between the parties or the date of agreement or amendment to an existing agreement between the parties.





# VMware Product Security

An Overview of VMware's Security Programs and Practices

TECHNICAL WHITE PAPER



## Table of Contents

Executive Summary .....	2
Software Product Lifecycle Management.....	2
Privacy by Design .....	3
Building Security into VMware Products and Practices .....	3
Product Security .....	3
Security Development Lifecycle.....	4
Planning.....	6
Design .....	6
Implementation .....	6
Validation .....	7
Security Review.....	8
Production .....	8
Security Response Center.....	8
Security Evangelism .....	9
Security Certifications .....	9
Software Supply Chain Security .....	9
Managing Supply Chain Risk .....	9
Industry Participation .....	10
Protecting Product Source Code .....	10
Code Integrity .....	10
Source Code Management.....	10
Secure Delivery .....	11
Issue Remediation .....	11
Providing Secure Product Support Services.....	11
Vulnerability Management .....	11
Penetration Testing .....	11
Conclusion .....	12



## Executive Summary

VMware, the industry-leading virtualization software company, empowers organizations to innovate and thrive by streamlining IT operations. Radically transforming IT with technologies that make your business more agile, efficient and profitable, VMware software powers the world's most complex digital infrastructure. The company's compute, cloud, mobility, networking and security offerings provide a dynamic and efficient digital foundation to over 500,000 customers globally, aided by an ecosystem of 75,000 partners. Our unique solutions drive outstanding application interoperability and customer choice, benefiting both business and society.

VMware understands that the integrity of its cloud services and products (herein "products") is of utmost importance to our customers and recognizes that unless its products meet the highest standards for security, its customers will not be able to deploy them with confidence. To achieve this, VMware has established oversight procedures that identify and mitigate potential product security risks during development and has instituted programs and practices that support both the development of secure products and solutions and drive security awareness across the enterprise. In response to risks to critical infrastructure, intellectual property, and sensitive information posed by the constantly evolving threat landscape, VMware has developed comprehensive and rigorous software security assurance processes and procedures that demonstrate the integrity of its products and address potential vulnerabilities.

This white paper provides an overview of how our commitment to building trust with our customers is present in every facet of our comprehensive, risk-based software assurance process and is reinforced in our program structure.

VMware's approach to product and information security addresses potential vulnerabilities within areas such as:

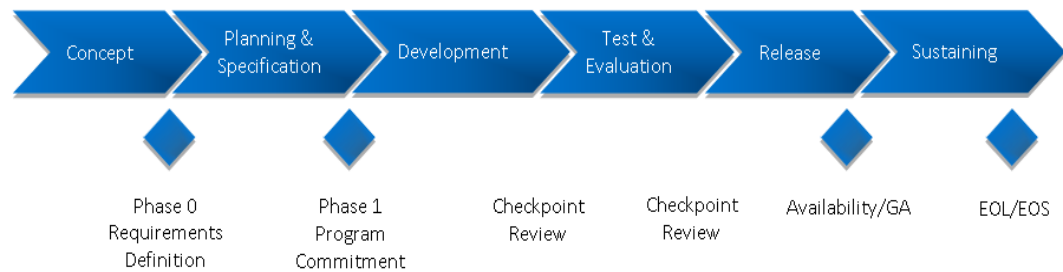
- Software product development
- Software supply chain
- Technology partnerships and ecosystems

## Software Product Lifecycle Management

The VMware Software Product Lifecycle includes the framework, governance, and set of executive checkpoint reviews, tools, artifacts, and guidance that enable VMware product business units (BUs) to ensure business readiness at the time of product availability and throughout the product lifecycle. Central to the framework is an integrated and predictable approach to product and cross-functional planning, release/program management, execution, measurement, risk management, and decision making at each phase of the product lifecycle.

The VMware Software Product Lifecycle provides the framework for addressing critical decision points as a product proceeds through the lifecycle phases from Concept to Sustaining state.





**Figure 1** Enterprise Product Lifecycle Management Workflow

## Privacy by Design

Building in appropriate security controls and safeguards in VMware products and services is integral to VMware's 'privacy by design' framework. The VMware security team and engineers work with the VMware privacy team during product development to evaluate security and privacy risks and implement safeguards to mitigate and minimize such risks and comply with applicable law. Further, as part of VMware's privacy program, VMware details the types of data collected in connection with its products and services in its [Products and Service Notice](#), and the types of data VMware collects and uses to manage accounts and customer relations in its [VMware Privacy Notice](#). The VMware Products and Services Notice contains information regarding the types of data collected and used in connection with VMware's provision of the Services.

## Building Security into VMware Products and Practices

VMware has established programs and practices that identify and mitigate security risks during and throughout the software development process. Through these activities, VMware delivers secure products and solutions for its customers.

Based on industry-recognized best practices and standards, and developed in consultation with trusted industry participants, VMware's programs and practices focus on:

- Building secure software
- Protecting the intellectual property related to software products
- Managing software security supply chain risks
- Managing technology partner and ecosystem risks
- Delivering secure product support

### Product Security

The Product Security group, VMware Security Engineering, Communications & Response (vSECR), develops and drives software security initiatives across all of VMware's R&D organizations to reduce and mitigate software security risks. Their goals and practices oversee a product development process that employs a comprehensive approach to assist in the delivery of secure products. The teams and efforts described in this section represent VMware's commitment to promoting a security-conscious approach and culture to foster positive cross-functional collaboration in security.





VMware has a comprehensive approach to security which includes collaboration with many teams across our organization, including Research and Development, Corporate Legal and Privacy, as well as Support and Field organizations. VMware also works closely with Industry Organizations, Security Analysts and Researchers, etc. to stay current on the Industry threat landscape and security best practices.

**Figure 2** VMware Product Security

The vSECR group develops and drives software security initiatives across VMware's R&D organizations to reduce software security risks. The vSECR programs and engineering functions include:

- **VMware Security Development Lifecycle (SDL)** – A comprehensive program to identify and mitigate software security risks during the software development lifecycle. The program is supported by a security engineering team that performs security design reviews and thorough security testing.
- **Security Response Center (VSRC)** – Leads the analysis and remediation of security issues in VMware products, once products have been released to customers.
- **Security Certifications** – A program to drive key products through appropriate security certifications such as Common Criteria, FIPS 140-2, and DISA STIG
- **Security Evangelism** – A program to raise security awareness and competency within the broader VMware R&D community through formal and informal training

## Security Development Lifecycle

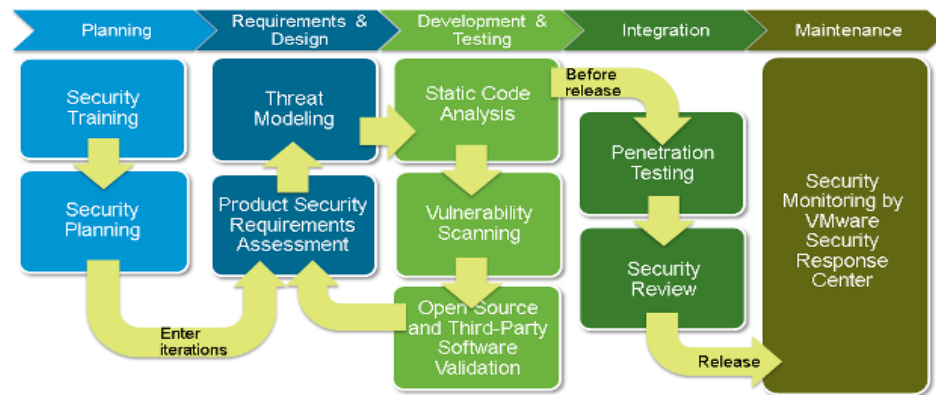
VMware's Security Development Lifecycle (SDL) program is designed to identify and mitigate security risk during the development phase of VMware software products. The development of VMware's SDL has been heavily influenced by industry best practices and organizations such as SAFECODE (the Software Assurance Forum for Excellence in Code) and BSIMM (Building Security In Maturity Model).

VMware is active in the broader software industry security community, becoming an early member of BSIMM in 2009 and a member of SAFECODE (Software Assurance Forum for Excellence in Code) in 2014, an organization driving security and integrity in software products and solutions. VMware is also active in the security research community and works to actively cultivate relationships in this community. For example, VMware brings speakers from the research community onto VMware campuses to present technical talks on security topics. Furthermore, VMware hosts annual 2-day internal security engineering conferences at multiple VMware facilities globally, where external security researchers and internal security experts from across the globe present.

VMware SDL is periodically assessed for its effectiveness at identifying risk and new techniques are added to SDL activities as they are developed and mature.



### VMware Security Development Lifecycle



**Figure 3** VMware Security Development Lifecycle

Current VMware SDL activities include:

- **Security Training** – vSECR maintains role-based technology-specific product security and privacy training curricula in VMware’s central learning management system.
- **Security Planning** –SDL planning early in the development lifecycle forms the basis for the later Security Review activity, when a product’s security profile is evaluated at development milestones.
- **Product Security Requirements Assessment** – This activity examines how a product adheres to VMware Product Security Requirements (PSR), which includes standards for:
  - Authentication
  - Authorization
  - Encryption
  - Certificates
  - Network security
  - Virtualization
  - Accountability
  - Software packaging and delivery
- **Threat Modeling** – This activity identifies security flaws and incorrect design assumptions present in the architecture of a product.
- **Open Source Software and Third-Party Software Validation (OSS/TPS)** – This activity highlights OSS/TP software components with known vulnerabilities so they can be fixed before being included in a product release.
- **Static Code Analysis** – This activity uses automated tools to detect defects and security flaws in code.
- **Vulnerability Scanning** – This activity uses automated tools to detect security vulnerabilities in running systems.
- **Penetration Testing** – This activity attempts to circumvent security controls and uncover implementation vulnerabilities in running environments.
- **Security Review** – This activity collects and examines the results of all the preceeding activities.

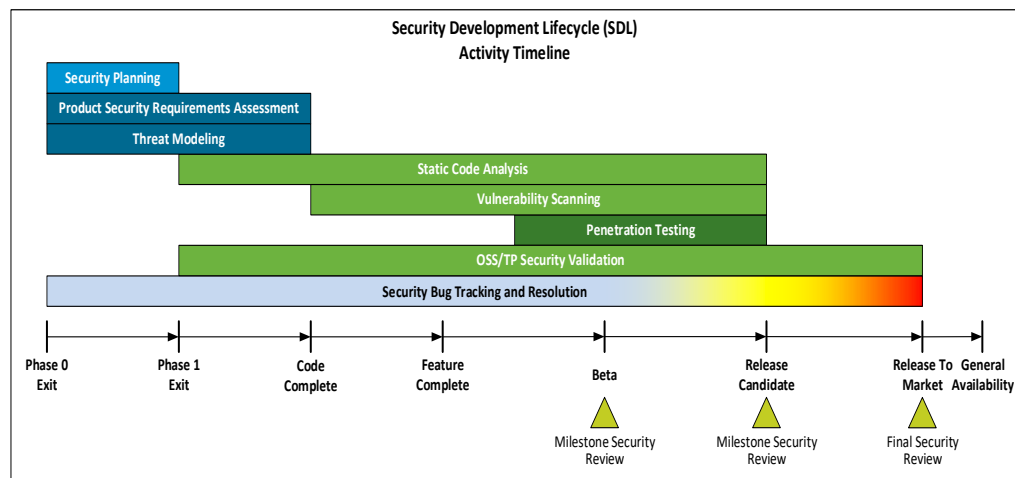
The vSECR group owns the definition and practice of SDL processes. The SDL is the secure software development methodology promoted by vSECR to help VMware product development groups identify and mitigate security issues early in the lifecycle so that their software is safe for release to customers.



The SDL's end-to-end set of lifecycle processes aim to help product development groups achieve these goals:

- Reduce their component's risk profile and attack surface
- Identify and remediate costly security-related design flaws early in the development process before much coding has taken place
- Discover and remediate security vulnerabilities prior to availability
- Educate their teams on security issues and security best practices

Figure 4 illustrates the timeline of SDL activities and product release milestones.



**Figure 4** vSECR Security Development Lifecycle (SDL) Activity Timeline

The SDL processes include these activity phases:

## Planning

During this phase, the development team documents its security plan (strategy, risks, initial schedule, etc.) for the release, utilizing the Security Development Lifecycle workflow.

As part of VMware's abiding commitment to ensuring support around security early in the development process, VMware offers courses for managers, developers, and quality engineers in:

- Security concepts
- Security design and testing
- Secure coding techniques for specific languages
- Various security tools

## Design

During this phase, the development team utilizes the VMware Product Security Requirements (PSR) to identify and remediate security issues in VMware products before release.

Additionally, the development team formally develops a threat model that identifies potential security flaws and incorrect design assumptions present in the architecture of a software application or component. Threat modeling occurs early in the development process, and thus allows adequate time for teams to remediate any design-related security issues.

## Implementation

During this phase, the development team utilizes automation tools as part of Static Code Analysis (SCA) to



detect defects, including security flaws, in software components that are not running or are "at rest".

Additionally, VMware requires that its development teams publish the names and release levels of each Open Source/Third-Party Software (OSS/TP) product or library that the team uses in building VMware products or components so they can update to the latest, fixed versions of the OSS/TP software in all product releases.

### **Validation**

During this phase, the development team employs automated Vulnerability Scanning processes to identify security vulnerabilities in computing systems running in a network to determine the specific ways the system can be threatened and/or exploited.

Additionally, the development team uses Penetration Testing (pen test) assessments to determine if a malicious intruder can successfully attack a software product or solution. VMware conducts these tests on an isolated, mock customer environment. The tests include reviews of the product architecture and source code, and utilize various commercial and/or custom vulnerability detection tools.

Lastly, during this stage, the Security Review is conducted to establish whether the subject software has undergone the required SDL activities adequately, and has addressed security risks such that the software is suitable for release to customers. Formal Security Reviews occur before the Beta, Release Candidate (RC), and Release to Market (RTM) milestones.



## Security Review

The Security Review establishes whether the subject software has undergone the required SDL activities adequately in order to identify security risks and addressed these risks such that the software is suitable for release to customers.

While the data that the Security Review evaluates is monitored throughout the entire security development lifecycle of the software, formal Security Reviews occur before the Beta, Release Candidate (RC), and Release to Market (RTM) milestones.

## Production

When a VMware product has reached the general availability milestone, the product enters the production stage of its lifecycle, and remains in production until it reaches the end-of-life milestone.

The VMware Security Response Center (VSRC) is charged with monitoring the landscape for all reports of security issues concerning VMware products.

The internal role of VSRC is to investigate reported vulnerabilities and provide information on security issues to the appropriate teams. VSRC serves as a point of contact for security researchers, customers, partners, and other external parties with a point of contact for reporting vulnerabilities in VMware products ([security@vmware.com](mailto:security@vmware.com)). **Note:** We encourage use of encrypted email. Our public PGP key is found at [kb.vmware.com/kb/1055](http://kb.vmware.com/kb/1055).

When VSRC detects or receives a report of an issue with a VMware product, VSRC works with the development team to investigate the issue. VSRC continues to coordinate the remediation and communication of the issue with the appropriate product and support teams. VSRC is additionally responsible for communication and dissemination of all relevant VMware Security Advisories. VMware Security Advisories can be found at <http://www.vmware.com/security/advisories/>.

## Security Response Center

Established in 2008, VSRC is responsible for managing and resolving security vulnerabilities in VMware products once products are released to customers. VSRC has a mature process for investigating reports, coordinating disclosure activities with researchers and other vendors when appropriate, and communicating remediation to customers via security advisories, blog posts, and email notifications. VSRC is well established within the security research community and participates in many external security events in order to foster strong working relationships with the security research community. For example, VMware participates in major security conferences such as RSA, Black Hat, DEF CON, and CanSecWest. Also, VMware is involved in the security community, including FIRST and ICASI, and hosts Moosecon, its own internal security conference, featuring internal and external speakers. VMware's security response policies are well established and are publicly documented on the VMware website at [http://www.vmware.com/support/policies/security\\_response.html](http://www.vmware.com/support/policies/security_response.html).



## Security Evangelism

The long-term goal of the Security Evangelism team is to increase the level of software security awareness and competency within VMware's R&D community. This allows the SDL process to scale effectively. The team uses several programs to achieve this:

- An R&D wide, role-based technology-specific online software security training program
- Participation as speakers at VMware's annual Research & Development Innovation Offsite (RADIO) conference
- Software security challenges, competitions, and hackathons focused on VMware products
- Moosecon, an internal 2-day VMware security conference that involves industry-recognized speakers from both academia and the security research community as well as speakers from within VMware

## Security Certifications

VMware has a long history of participating in FIPS and Common Criteria standards with the first VMware cryptographic module validated in 2007 and first VMware product being certified in 2008. The Security Certifications team drives the certification of major VMware products as well as the validation of cryptographic modules used in those and other products. The team, also, actively participates and contributes in the development of the standards and various Protection Profiles by continuously engaging with various WGs/TCs/ITCs.

For a complete list of VMware's Common Criteria certified products, visit <http://www.vmware.com/security/certifications/common-criteria.html>

For a complete list of VMware's FIPS 140-2 validated modules, visit <https://www.vmware.com/security/certifications/fips.html>

## Software Supply Chain Security

With global expansion of the software industry, security concerns have increased that a product or service could be compromised by malicious code introduced during product development or maintenance. Technological innovation and changes in sourcing and supply chain strategies have made software supply chain security a global challenge. Threats ranging from risks associated with using third-party code and open source components to IP theft have dramatized the vulnerability of this new risk domain. VMware is actively engaging in proactive measures to minimize the occurrence of these risks and has launched several initiatives to address the security of our supply chain.

### Managing Supply Chain Risk

VMware utilizes a Supply Chain Risk Management program that focuses on secure sourcing and hardware, firmware, and software integration relating to building solutions. It includes use of an approved vendor list for several of its BUs and functions.

- VMware's recycle program for hardware products addresses supply chain risk by securely recycling equipment that may hold information sensitive to the supply chain. For example, hard drives that are at end of life and were used in the source control systems are properly recycled to ensure that the data from the source control systems is removed.
- VMware has established processes around partnerships with entities deemed to be of increased supply chain risk and around the sharing of source code with third-parties
- With respect to partnerships, VMware has an established process to determine if a partner is



considered to be of increased security risk. If a partner meets certain criteria, they may be excluded from certain programs that permit direct access to VMware IP.

- Both inbound and outbound contracts with software supply chain security implications are reviewed by the Legal and Product Security teams. VMware includes terms that set minimum software security standards in its OEM (Original Equipment Manufacturer) and third-party software license agreements that are in keeping with or exceed industry best practices.

## Industry Participation

VMware is active in the broader software industry security community. As mentioned earlier, VMware is a participant in the BSIMM process and a member of the SAFECode organization. VMware is also active in the security research community and works to actively cultivate relationships in this community. VMware also actively engages with the Open Source community through contributions to existing community-based projects as well as developing, releasing, and leading new open source projects and initiatives.

## Protecting Product Source Code

Product source code managed by the Source Code Management (SCM) team follows processes designed to safeguard the integrity of VMware's product-related intellectual property while providing engineers access to source code required to develop and maintain its products. Also, the SCM team manages the source code systems environments.

## Code Integrity

These controls can allow for code integrity problems to be identified and remediated in a timely manner for perpetual software.

**TABLE 1 CODE INTEGRITY CONTROLS**

Control	Current Process
Code review	Well-adopted practice within teams
U.S.-Based Builds	All products TAA compliant
Security Reviews	Security Reviews conducted prior to release
Risk Management of Open Source Software (OSS)/Third-Party Software (TPS) supply chain	Contract provision to allow security testing of TPS

The following sections describe processes aimed at supporting product integrity for a VMware product that achieved Common Criteria Certification. The process extends to other VMware products.

## Source Code Management

Source code control protects the security and integrity of code that is written, developed, tested, and evaluated. Source control covers code creation, modifications, deletion, and incorporation of the code into larger parts. Audit controls within the source control system automatically track what changes have been made, who made them, when a change was made, as well as other consequences of those changes. Access to the source code is controlled by a network access and is controlled on a per-user basis, by means of user permissions and roles.

The product source code is stored on centrally managed servers in a secure area and protected behind a network firewall.



## Secure Delivery

Several procedures are necessary for VMware to maintain security when distributing the product to a customer's site. For a valid delivery, the product received must correspond precisely to the product master copy, without tampering, or substitution of a false version. The delivery procedures ensure that the integrity and authenticity of the product are maintained and that they are verifiable by the customer and by VMware after delivery has been completed. The product is delivered via VMware's websites by electronic distribution only. The end user is supplied with the product, product documentation, and product license.

## Issue Remediation

Customers report security issues to VMware's Product Security group ([security@vmware.com](mailto:security@vmware.com)) when a problem is encountered in the normal operation of the product. Product issues are also reported, captured, and filed through VMware's Global Support Services (GSS). Internal wiki pages are used to track security related bugs reported from the [security@vmware.com](mailto:security@vmware.com) mailing list.

Any bug discovered during product development, design change, testing, or by a customer must be triaged, documented, and a solution offered before the bug report can be closed. These bugs include suspected and/or confirmed security flaws.

## Providing Secure Product Support Services

VMware's Global Support Services (GSS) organization is global and as part of standard practice engages the necessary resources wherever they are in the world. VMware has established a variety of process and procedures to protect data while working to resolve customer support issues. For a more in-depth overview of Global Support Services and more on their expertise in Virtualization and Cloud Infrastructure, see <http://www.vmware.com/files/pdf/support/VMware-Support-GSS-BR-EN.pdf>.

## Vulnerability Management

VMware has a Vulnerability Management program backed by approved and tested policies and procedures. Vulnerability scans are performed regularly on VMware developed products and Cloud Services.

System and application owners are required to address critical and high vulnerabilities with a plan of corrective action. Responsiveness requirements are dependent on vulnerability severity.

Risk analysis and acceptance are performed on vulnerabilities to confirm the vulnerability, and to determine the appropriate means of addressing the vulnerability. Senior management within the applicable BU – as well as IT and Information Security senior management – are required to approve the existence of all risks associated with vulnerabilities that are not patched with vendor provided fixes.

## Penetration Testing

VMware utilizes trained and experienced internal security engineering staff to periodically perform penetration testing of critical systems and applications. Findings from penetration testing are handled in the same manner as vulnerabilities as discussed above. Penetration test results are considered VMware Private/Protected information and are not shared outside of the organization.

In order to achieve more meaningful test results, VMware uses both white and gray box testing. A gray box approach is a mixture of black box and white box testing. White box testing means that all the source code will be made available and black box testing means that the actual pentest will be performed without any source code access. The gray box method enables the security engineer performing the pentest to have source code available to assist with penetration testing. This results in a more robust set of tests because the penetration testers can achieve deeper and broader access since they spend less time breaking into targeted assets.



## Conclusion

VMware strives to build products that its customers trust in the most critical operations of their enterprises. To promote this, VMware has established oversight procedures that identify and mitigate potential product security risks during development and has instituted programs and practices that drive software security initiatives and awareness across the enterprise.

VMware's focus on product security strategy and our security development lifecycle ensure our ability to continuously protect sensitive customer information from product vulnerabilities.

In closing, this document represents VMware's innovative, cooperative approach to security for its world-class virtualization software products and solutions. As such it also represents VMware's continuing commitment to its customers' success.





**VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 1-877-486-9273 Fax 650-427-5001 [www.vmware.com](http://www.vmware.com)**

Copyright © 2019 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.  
VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.





# Information Security Management at VMware

This document contains descriptions and key elements of VMware information security policies.



## VMware's Commitment to Information Security

Information security is important to VMware. VMware is committed to protect the integrity, confidentiality, and reliability of VMware information and information systems from unauthorized disclosure, removal, acquisition, modification, or destruction. VMware's information security service management and VMware information security policies are the foundation for the security of VMware information assets and VMware's obligation to its customers regarding information confidentiality, integrity, and availability.

## VMware's Information Security Organization

VMware has a designated Chief Security Officer to oversee information security for the enterprise. Multiple groups within VMware have a role in establishing, maintaining, monitoring, and operating security practices, including: Incident and Vulnerability Management, Security Operations, Information Security Governance, Risk and Compliance, Legal, and Internal Audit.

Service management has been established to ensure the right processes, technologies and service owners are in place to deliver, manage, and improve VMware information security services. VMware personnel have an obligation regarding the protection of information in accordance with VMware Information Security policies.

## About Information Security Policies @ VMware

VMware strives to achieve a high level of information protection standards. Relevant policies for information security have been established that are in line with VMware corporate objectives and in accordance with business requirements, relevant laws and regulations, contracts, and current or projected security threats.

Based on international standards ISO/IEC 27001 and consistent with industry-accepted practices and security frameworks, VMware information security policies define requirements for the protection of VMware information and information systems. These policies apply to all personnel who manage, use, or have access to VMware information assets, as well as to all VMware information assets and information processing environments including those infrastructures and services used to support VMware Cloud Services.

## Policy Oversight – VMware's Policy Executive Committee

All policies are required to have an Executive Owner who is a Vice President level or above. The Executive Owner approves the policy as well as any changes to the policy and ensures that the policy is reviewed and updated at least annually.

VMware's Policy Executive Committee has been established since 2016 to oversee new and significant changes to policies at VMware, as well as promoting compliance to those policies. Membership consists of fifteen (15) executives (Vice President level or above) representing various business lines from across the company including Information Security, Legal, Compliance, Finance, Human Resources, and Internal Audit. At a minimum, this committee meets semi-annually.



## VMware Information Security Policies

Below lists and describes the policies implemented by VMware for establishing, implementing, maintaining, and continually improving information security.

VMware security practices are in line with many leading industry standards. The policies and practices referenced herein reflect a baseline standard and is intended to provide general confirmation of the implementation of such standards across the VMware business.

**! Note:** Specific policies implemented by VMware that are described herein are confidential and are not publicly available.

---

### Information Security Governance Policy

As the overarching policy, this policy governs information security at VMware starting with the company's commitment to information security. This policy defines the baseline for establishing an information security program, policies, and practices, as well as mandatory requirements for training and compliance. Roles and responsibilities are designated, and VMware's key information security principles are defined, including:

- Secure by design
- Defense in depth
- Least privilege
- Segregation of duties
- Risk and value-based security controls
- Control standardization and automation
- Auditability
- Independent review

### Acceptable Use Policy

This policy requires that information and information resources are used appropriately by VMware personnel. Monitoring of information systems is established where necessary for business purposes. Compliance with corporate policies is required for all users, including but not limited to VMware's "Statement of Policy on Equal Employment", "Prohibited Harassment Policy" and "Business Conduct Guidelines". VMware's core values include:

- Acting with integrity
- Avoiding conflicts of interest
- Complying with insider trading restrictions
- Respecting and protecting the personal information of others
- Complying with antitrust and competition laws
- Obtaining and handling trade secrets and confidential information of others with care
- Being mindful of trade control and anti-boycott laws
- Protecting confidential and proprietary VMware information
- Ensuring full, fair, accurate, timely, and understandable disclosure and financial reporting
- Complying with applicable laws and guidelines regarding records retention

### Incident Management Policy

VMware has established this policy to ensure the critical elements of the incident lifecycle are managed in a structured manner. The policy and associated procedures address the key elements of incident response, such as the handling, monitoring, and reporting of an information security incident, and forensics and remediation after an incident occurs, as relevant and applicable. Any suspicious or unusual activity must be reported to the incident response team. This policy and associated procedures align with the data breach requirements mandated by the global regulatory requirements of VMware office locations.



## Access Control Policy

This policy ensures system access and privileges to VMware information resources is managed to minimize risk, commensurate with the business need. System access is granted on a 'need-to-know' basis and for legitimate and authorized VMware-business needs. Segregation of duties is applied to privileges granted. Requirements are established for appropriate authorization, user access provisioning, change of access rights, access suspensions and terminations, inactive accounts, management of privileged access, and access revalidation.

## Authentication & Password Policy

VMware has established this policy to enable authentication mechanisms to protect access to VMware information assets. Key elements of this policy include the secure logon procedures, password configuration (complexity, restrictions for accounts, and testing), password administration, and user responsibilities for authentication (safeguarding authentication information and reporting compromised authentication).

## Encryption Policy

This policy provides VMware's encryption requirements to support the protection of information, covering both data-at-rest and data-in-motion. In addition to the required applications for encryption, key elements of the policy include encryption methods, secure cryptographic key management, and defined roles and responsibilities for maintaining compliance to essential cryptographic standards. VMware establishes cryptographic controls in alignment with relevant agreements, laws and regulations, including, restrictions on import/export of hardware or software with cryptographic capabilities, use of encryption to achieve information security objectives, and mandatory or discretionary methods of access. Cipher strengths in use at VMware are based on, at a minimum, industry standard practices.

## Business Continuity Policy

This policy governs VMware's corporate business continuity program. Requirements are specified to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence of, prepare for, respond to, and recover from disruptive incidents when they arise. Periodic business impact assessments drive business continuity plans for disaster events that would disrupt essential business operations, involve, or affect VMware personnel, office buildings or data centers, such as natural disasters, fires, floods, power disruptions, or any information security event compromising VMware's critical business services. This policy applies to all VMware users who manage or operate VMware systems or business services.

## Infrastructure Security Policy

In this policy, objectives for VMware infrastructure are defined in adherence to information security protocols designed to ensure that networks and associated applications and systems are managed and monitored in such a manner as to prohibit unauthorized access. This policy governs the maintenance, management, and ongoing improvement of network security practices. Controls are established for provisioning network connections, private network services, value added networks and managed network security solutions, such as firewalls and intrusion detection systems. Key elements of this policy include network controls, network configuration, and change management (segmentation, default deny, firewalls, audits), connections, IP address & subnet management responsibilities, and protocol policies.



## Production Control Policy

Under this policy, VMware implements restrictions on production environments such as requiring production be separated from both development and test environments. As well, standing permission to change, update, or add to production data is prohibited; production data can only be altered using formal change management processes. This policy confirms that production data is not to be used in test or development environments unless appropriate security measures are taken, such as data scrubbing, consistent with applicable law and contractual obligations.

## Change Management Policy

This policy ensures that a systematic framework is used for the documentation, testing and evaluation of all proposed changes to VMware's production environments. This policy ensures that mitigation of risks that could threaten stability, resiliency, security, regulatory compliance, and availability of VMware's production applications and infrastructure are addressed. This policy is applicable to all changes made to IT production environments. Key elements of this policy include requests for change, review and analysis, approval, communication, implementation (test, implement, post implementation review), fall back / roll back, and emergency changes.

## Backup Policy

To protect against loss of business-critical information and ensure continuous availability, this policy establishes data backup scheduling, testing, retention, and protection requirements for VMware production systems. Adequate backup accommodations are established to ensure that essential information and software can be recovered quickly following a disaster or media failure.

## Logging & Monitoring Policy

This policy establishes proactive measures to effectively log and monitor information system activities for the purposes of providing service assurance and preventing the exploitation of VMware information and information systems. Logging and monitoring help VMware to improve its security posture through the collection of system behavior. Log protection as well as controls around the logging and monitoring tools help to ensure the integrity of the data. Additional requirements include individual accountability, reconstruction of events, intrusion detection, and problem identification. This policy also provides guidelines for operational logs, error logs and security event logs that shall be maintained and reviewed for all critical operations and systems.

## Operations Security Policy

This policy ensures standardization of operational security throughout VMware's IT environment and ensures critical operating procedures are documented and maintained. Additionally, this policy provides requirements to ensure enterprise anti-malware software installation on development, domain, and production devices owned and operated by VMware which hold VMware information, passwords, or keys. VMware information is not to be stored on devices where anti-virus software is not maintained.

## Vulnerability Management Policy

This policy enables VMware to take measures for the discovery, evaluation, remediation, and management of vulnerabilities that affect VMware's information systems, information, or business processes. The policy applies to systems (devices, network devices, security devices) and applications (servers, database, custom and commercial applications) owned, managed, or operated by VMware. Key elements of this policy include identifying threats, vulnerability scanning and assessment, monitoring, patches (scheduling), reporting, and remediation.



## Asset Management Policy

Designed to ensure that company technology assets are identified, inventoried, and assigned a designated owner who has responsibility for its management and control over the asset lifecycle. This policy requires secure practices related to asset management including the return of assets, removal and security of any off-site assets, and secure disposal of assets.

## End User Device Security Policy

VMware has established this policy to minimize the risk of vulnerabilities presented when end user devices are used to access and use VMware information and information systems. Users are expected to ensure device security requirements (screen locks, passwords, anti-malware protection, encryption, idle-time passwords, and backups) outlined in this policy are followed. VMware has defined backup standards for staff devices that complement this policy. Other key elements of the policy include compliance requirements for all users, return of assets upon termination, mobile device management software, and maintenance and care of mobile devices.

## Data Classification Policy

This policy defines VMware's approach to data classification, and outlines responsibilities for ownership, labelling and secure handling. VMware implements secure data handling and protection standards at all stages of the data lifecycle (which includes data transmission, storage & disposal) to protect the confidentiality, integrity, and availability of data consistent with the assigned classification.

## System Acquisition, Development & Maintenance Policy

This policy requires that information security is incorporated across the lifecycle of information systems at VMware, including project management, system development, system enhancement, and system acquisition. Key elements in this policy include use of change control for deployment of information systems, restricted & secure access to program source code, use of open-source software, information security for new or enhanced systems, secure system engineering principles, outsourced development, and system security and acceptance testing. This policy is supplemented with Information Security Architecture Principles, Information Security Architecture Principles for Cloud, and Platform & Application Security Standards.

## Security Compliance Policy

This policy requires the identification of applicable legal, statutory, regulatory, and contractual requirements related to the security of information at VMware. Controls and individual responsibilities to meet these requirements are defined. This policy requires protection of corporate security records, and regular compliance reviews and audits of VMware information and information systems.

## Human Resources Information Security Policy

This policy is designed to ensure that the risks of personnel error, theft, fraud, and misuse are prevented or mitigated with appropriate hiring practices. The policy includes VMware's background screening practices upon hiring, requirements for the terms and conditions of employment, and required disciplinary processes for information security breaches.



## Physical Security Policy

This policy governs the safeguarding of offices, datacenters, support centers, and other business premises/locations globally. It establishes the requirements necessary to physically secure VMware facilities, incorporating physical and environmental security measures to minimize risk, avoid threats, and eliminate vulnerabilities to protect information systems and staff. Key elements of this policy include perimeter security, physical entry controls, physical access controls, preventing misuse of facilities, protection against external and environmental threats, access to restricted areas, delivery and loading areas, supporting utilities, and clean desk/clear screen.

## Third Party Risk Management Policy

Ensuring the security of VMware information and information systems is not reduced when working with third parties, this policy establishes requirements for managing risk where third parties may have access to VMware's non-public information. Sourcing and business teams collaborate with information security risk to ensure a risk-based approach is taken with respect to all third parties to ensure the security of information assets. This policy defines the requirements for assessments to be performed as part of negotiating and reviewing third party agreements in line with VMware information security objectives and ongoing monitoring of such third parties for compliance. VMware vendors/suppliers do not have access to customer data/information unless required by a particular service offering.

---

## Revision History

DATE	CHANGES	MODIFIED BY
August 2018	Document approved by VMware legal for external distribution and publication	A Singh
June 2020	Document approved by VMware legal for external distribution and publication	D Wylie
October 2021	Document approved by VMware legal for external distribution and publication	D Wylie





# Global Resiliency Program

VMware is a provider of virtualization and virtualization-based cloud infrastructure solutions. Our solutions address a range of IT issues, including facilitating access to cloud computing capacity, business continuity, software lifecycle management, and corporate end-user computing device management. Our solutions are organized into three main product groups: cloud infrastructure and management, cloud application platform, and end-user computing.

VMware developed a global resiliency program that outlines how we respond to events that threaten to disrupt our business. While every business disruption poses unique problems based on external factors (for example, time of day or month, severity, nature of disaster, or geographic impacts), we are committed to our customers and doing what it takes for us to deliver the same quality service for which we're known.

Our resiliency program identifies what preparations must be made in advance of a disruption, as well as the steps to be taken when an event occurs. The program is reviewed periodically to determine the most critical business processes and the resources—people, equipment, records, computer systems and office facilities—required for operation. All documented resiliency plans and processes follow an annual standard maintenance and assessment schedule.

There are an incalculable number of events or circumstances that could result in a significant business disruption, and their impact may vary in size, scope, duration, severity and geographic location. Significant business disruptions may result in degrees of harm to human life and regional/national infrastructure (such as power, transportation and communications), which could impact VMware's recovery efforts.

While diligent in our efforts to plan for unexpected events, it is impossible to consider every possible scenario and develop detailed responses to each. VMware, in our sole discretion, reserves the right to flexibly respond to any disruption in a situation-specific and prudent manner. This document is not intended to provide a guarantee or warranty regarding the actions or performance of VMware, our computer systems or our personnel in the event of a significant business disruption. This information is provided solely to our customers and vendors. No further distribution or disclosure is permitted without our prior written consent. No person other than our customers and vendors may rely on any statement herein.



In the event of an actual declared disaster (including a force majeure event) and such disasters not fully addressed in the company's business continuity/disaster recovery plans, VMware will use commercially reasonable efforts to restore service to our customers as quickly as possible.

## Key aspects of the resiliency program

### Business continuity management

The business continuity management (BCM) program is under the direction of the chief information officer. The BCM steering committee—comprised of executive management across all lines of business—meets quarterly to review the overall program and provide any direction needed. Business continuity plans are developed and maintained to support the adequate performance of critical business functions. Business continuity plans and the business impact analysis are updated at least once per year to address major operational changes.

### Disaster recovery

VMware has a backup data center located in a different geographic location than the primary data center. In the event of a disaster, critical functions will be recovered at the alternate location. This enterprise-grade data center is secured with restricted access; has redundant uninterruptible power supply units; and is monitored for temperature, humidity and other environmental conditions. Disaster recovery exercises are conducted each quarter.

### Crisis management/crisis communications

VMware has emergency preparedness plans that provide additional emergency response, preparedness, instructions and guidelines to protect the safety and well-being of our employees and guests in the event of major disruptions and emergencies. Once activated, the crisis management team—comprised of select executives and senior managers from key departments—evaluates the severity of the event and responds accordingly.

### Exercise and maintenance

VMware conducts exercises to identify gaps in documentation or processes. Exercise findings and areas identified as requiring attention are documented and assigned to the appropriate subject matter experts for resolution.

### Staffing

All employees will be dedicated to restoring customer services as quickly as possible after a disruption. Teams are located globally and can continue operations if their primary offices are unavailable. Procedures are also in place to relocate employees, if needed.

### Pandemic planning

Aligned with World Health Organization guidelines, a plan has been implemented across the enterprise to address pandemic concerns.





# VMware Trust & Assurance

TECHNICAL WHITE PAPER





## Table of Contents

Introduction .....	2
Reliability .....	2
Performance .....	2
Evangelism and Education .....	3
Research .....	3
Field Engagement .....	3
Quality .....	4
Integrity .....	4
Release Management .....	4
The VMware Software Development Lifecycle (SDLC) .....	5
Ongoing SDLC Dynamics .....	6
Release Life Cycle: Metrics .....	6
Release Life Cycle: Readiness .....	6
Compliance & Cyber Risk Solutions .....	7
Software Supply Chain Security .....	7
Managing Supply Chain Risk .....	7
Privacy .....	8
Security .....	8
Product Security .....	8
Security Development Lifecycle .....	8
Security Response Center (VSRG) .....	9
IT Information Security .....	9
Commitment .....	11
Managing Critical Customer Issues .....	11
Ecosystem Services .....	12
Customer Advocacy .....	14
Customer Advocacy .....	14
VMware Global Support .....	14
Conclusion .....	15
Appendix .....	16
Privacy Resources .....	16
Certifications .....	16
More Information .....	16



## Introduction

As an industry-leading virtualization software company, VMware appreciates that the integrity, reliability, and security of its products are of utmost importance to its partners and customers.

The relentlessly advancing threat landscape over the last few years has yielded unprecedented cyber exploits which not only pose acute potential risk to critical infrastructure, intellectual property, and sensitive information, but can also erode a company's reputation. VMware is addressing the environment we now live in with innovative programs designed to get ahead of these problems and anticipate threat trends, along with keenly crafted assurance practices that engender customer trust.

VMware understands what matters to today's customer and is committed to furthering our insights through our well-established, candid customer dialogue and our growing transparency about the measures we take to ensure that our products and services continue to meet and exceed expectations on quality, performance and safety.

The VMware Trust and Assurance framework was created to drive this initiative of preserving and enhancing the trust customers place in VMware, our products and our services. We define trust as the demonstrable ability to execute on our commitments consistently over time—it is transparent, integrated, and proactive. Likewise, we are eager to communicate our proactive approach to reducing our risk landscape as well as activities ranging from development to security in support of providing comprehensive assurance—or proof—that our product offerings are secure, reliable, high quality, and trustworthy. This white paper discusses the teams, programs and practices that represent VMware Trust and Assurance's guiding principles of reliability, integrity, security and commitment.

## Reliability

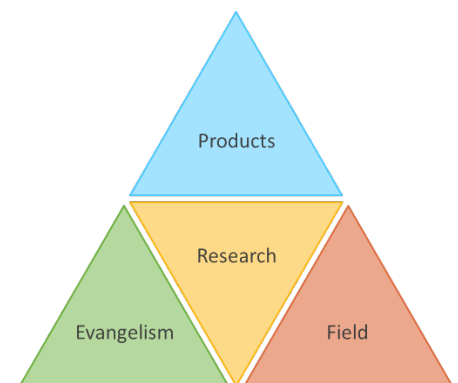
Quality and performance are key stakes in today's Infrastructure software and services. Our virtualization offerings have earned renown for high quality and high performance. In fact, we have led the creation of industry virtualization benchmarks for measuring workload performance. We take proactive measures to ensure we stay ahead in the area of both quality and performance to ensure our customers can continue to rely on us as we move into the next generation of virtualization software and cloud-based services.

## Performance

The Performance Engineering team's mission is to ensure that VMware products and solutions perform competitively and scale optimally. As critical contributors at every stage of the product lifecycle, this team cultivates a culture where everyone owns performance as an ongoing key differentiator from on-premise to hybrid cloud to end user solutions. This aim is driven by core performance engineering values, which are commitment, collaboration, curiosity, customer focus, and excellence. These principles are illustrated in each of the Performance team's four main areas of focus: products, research, evangelism, and field.

For product performance, the team works to ensure VMware products and services perform excellently and scale optimally. Performance engineers:

- Ensure new products are architected and designed to perform
- Drive performance improvements for VMware products





- Evaluate progress across releases and competitors
- Prototype and develop product performance enhancements

A component of this effort is improving product performance via improved tier 1 application performance and relentless demonstration that all workloads virtualize. Improving performance also means opening new market opportunities, such as creating low latency for financials and online game hosting, as well as providing improved management product performance.

### Evangelism and Education

The Performance Engineering team is committed to evangelizing and educating on Performance practices across the entire VMware ecosystem and beyond by developing and driving benchmarks, including industry leader and a cloud-based benchmark. The team teaches “The Performant Way” to VMware developers, partners, and customers, which results in everyone’s enablement to own performance via practical guidance, which consists of 15 crisp examples across architecture, design, and test. This includes:

- Extending performance knowledge internally and externally
- Driving performance best practices into VMware products
- Developing leading cloud and virtualization benchmarks
- Engaging through VMworld, blogs, and internal and external conferences

### Research

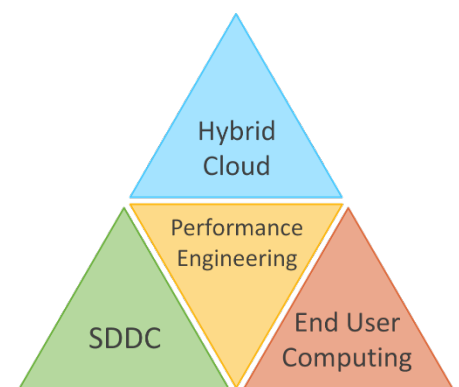
Performance Engineering embodies a major component of the “R” in R&D at VMware. Exploring and researching opportunities for improvement and innovation in collaboration with developers, universities, and industry groups, this team drives deep-dive investigations into products and features. These relationships with thought-leaders and academics enhances this team’s exploration of emerging technologies and innovations with performance impact. Research likewise informs the development of tools and visualizations for analysis and revelation, illustrated by this team’s growing library of patents, papers, and publications, including twenty-five patent applications in 2014 alone.

### Field Engagement

Another key vector that the Performance Engineering team pursues is enabling customers, partners, and VMware communities with performance expertise. This team facilitates VMware pre-sales by providing white papers, blogs, and hero numbers, and supports customers post-sale for the more complicated performance problems.

Performance Engineering continues to optimize IT outcomes across all products in the software defined datacenter (SDDC) with performance scorecards for every product. The team develops tools for sizing and analysis, and draws heavily on metrics with end-to-end impact across development, test, and integration. Their outcomes are also advanced by emerging research and differentiating technologies.

End User Computing is supported by improved desktop and mobile products, technologies, solutions, and benchmarks. Additionally, the Performance team is expanding virtualized desktop capabilities, such as EUC and ESX, and is exploring new technologies such as vCUDA, 3D, and containers.





## Quality

Quality has always been a bedrock principle for VMware. Ensuring that our customers deploy new releases and updates in confidence, and all VMware products reliably interoperate as expected are key facets of our quality vision.

VMware has a quality process in place for each of our software products consisting of test plans, test designs, test procedures, and test exit criteria. These documents are updated and revised for each new version and serves as the plan of record for the project. Requirements and designs are documented and tracked as part of the software development lifecycle process. Multiple phase checkpoints during the development lifecycle that require stakeholder sign-off of quality criteria are conducted to ensure that the program is tracking to plan and if adjustments are needed, they are assessed and implemented accordingly. Always conscious of customers' perspective, quality teams are focused on root cause analysis of customer issues. VMware strives for continuous process improvements, and tracks metrics for product release against prior versions of the product.

VMware has training programs in quality that include bootcamp and refresher training for all quality test engineers. The entire R&D organization has specific training for employees on standard tools and processes.

Independent internal audits, reviews and checkpoints are conducted company wide, encompassing products and processes. Code reviews are conducted as part of the software development process, and reviews and checkpoints are conducted at various milestone points to ensure that entry and exit criteria are being satisfied.

In a continued effort to strengthen its customer-centric perspective, VMware has also created a quality effort team, which works to understand quality issues at VMware, and consults with teams across the enterprise to get an in-depth understanding of what quality means to VMware customers. Examples of this collaboration include working with Customer Advocacy to understand the customer view of quality, and conferring with the Global Support Services (GSS), Continuing Product Development (CPD), and Ecosystems teams to understand their quality concerns and review their metrics and processes. The Quality System team closely works with R&D teams to review processes and metrics and provide feedback, and reviews industry quality standards like CMM. Accordingly, this team works to improve quality through process changes within R&D, GSS, and CPD teams, tracking releases using predictive metrics, and sharing quality practices.



## Integrity

Our software is developed, built, and delivered with integrity so that our customers, who include all of the Fortune 100, continue to entrust critical workloads to VMware. Our rigorous software development lifecycle and release management ensure product readiness and consistency, while our Compliance and Cyber Risk Solutions program helps customers foster a compliant-capable, audit ready posture. We manage Supply Chain security issues through a program that addresses risk associated with the use of third-party code and our IP sharing practices.

## Release Management

The Release Management (RM) team's mission is to drive product teams through efficient and measurable Software Development Life Cycle (SDLC) processes to deliver high quality product releases that implement the company goals for Suite and Cloud. RM works with all business units and all cross-functional groups and is responsible for delivering all VMware releases, which exceed 400 each year. As the team is centrally



hosted, it is optimally situated to drive consistency in release execution and in process compliance, maintain independence in status reporting and in escalation paths, and embed with engineering and quality teams.

RM provides active project management of VMware product releases, which includes driving product teams to build and release high quality products and services, using metrics to measure progress and to ensure release compliance to quality standards. RM additionally drives reporting and visibility on the state of releases and the release portfolio. Broadcasting metrics-driven release status updates provides invaluable information for the organization to stay at a competitive vanguard, while highlighting issues that require attention ensures the product or service is in an optimal condition before it is released.

RM establishes and improves release process best practices, and works with product teams to increase adoption of and consistency around release processes. It maintains the readiness of the product checklist, which ensures release compliance with legal requirements (open source, EULA, export compliance, country-of-origin, etc.), as well as ensuring compliance with accounting standards and federal certifications. For more information on our federal certifications, please see the VMware Product Security white paper at <http://www.vmware.com/files/pdf/VMware-Product-Security.pdf>.

### **The VMware Software Development Lifecycle (SDLC)**

The VMware SDLC defines a clear and repeatable process and creates a structured and organized execution that helps enable us to deliver secure, high-performing products, services, and solutions. The SDLC integrates best practices into the development process so that developers can focus on creating innovative products. It spans the product lifecycle end-to-end, and includes:

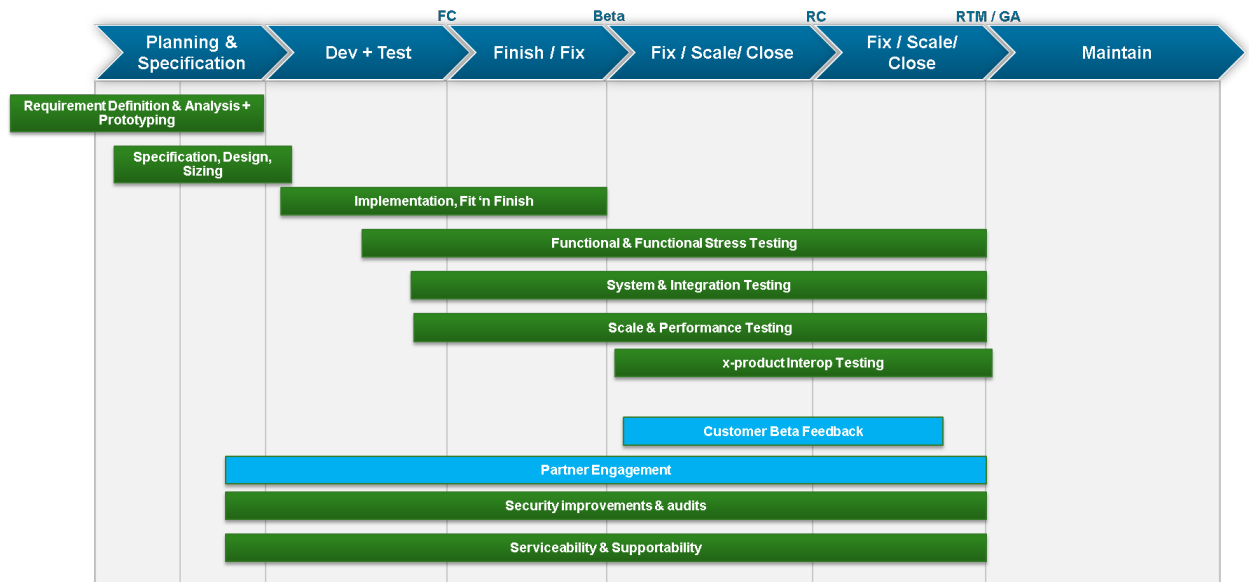
- Requirements and product definition
- Development
- Testing
- Legal requirements
- Documentation
- Security
- Performance
- Globalization and Localization
- Release
- Supportability
- Pre-release user testing, including dogfooding (VMware-internal hands-on usage), alpha testing, and beta testing

SDLC processes are executed by cross-functional release teams, and operate following either an agile/scaled agile or waterfall methodology. The processes are:

- Agile, mostly scrum for small and medium-sized product teams
- Waterfall for larger product teams

Oversight is exercised at multiple stages of release planning and execution, and the executive team is actively engaged in approving transitions between release phases.





Release Lifecycle: Key Activities

## Ongoing SDLC Dynamics

Current SDLC dynamics reflect the fact that increasingly, teams are looking for ways to accelerate their release cadence and are likewise working on transformations to deliver SaaS. Some SaaS teams are also adopting continuous delivery approaches, deploying smaller increments of capability at a higher frequency (weekly, daily).

## Release Life Cycle: Metrics

A powerful tool for communicating and planning, metrics can provide valuable insight into processes, goal attainment, and what the future may hold. At VMware, metrics are at the center of tracking, reporting on and making decisions on releases. Metrics and related goals (release criteria) are locked down as part of release planning, and criteria are defined for each key release milestone. Metrics and criteria are defined by area:

- Testing (Functional, System/Integration, Functional Stress, Interop)
- Scale
- Performance
- Security
- Readiness for Support / Maintenance

## Release Life Cycle: Readiness

Finally, prior to release, product/service increments need to comply with a number of mandatory readiness and compliance aspects. Product engineering teams are directly responsible for ensuring this compliance by taking action throughout the release cycle, and audits are conducted at various intervals in the release cycle to validate compliance. Key readiness aspects for product releases include:

- Security compliance
- Open Source license compliance
- EULA / Copyright / Trade Export Compliance
- Globalization / Internationalization
- Usability review
- Accessibility / 508c compliance
- Training / knowledge transfer to field and support personnel



## Compliance & Cyber Risk Solutions

Today's government and business executives are familiar with the benefits that come from improving their information technology operations by using server virtualization when moving to the cloud. Those benefits--the ability to respond rapidly, isolate applications from one another during a cyberattack, and maintain business continuity while keeping resource costs low--have been proven. However, executives chartered with maintaining continuous compliance practices continue to be concerned about managing risk, particularly in regulated environments, such as PCI, FedRAMP, FISMA, HIPAA or CJIS.

Assessing risks and then developing adequate controls can be difficult in evolving environments. With complexity comes rising costs: the costs of audits and remediating the findings; the longer time needed to develop and implement new offerings; and the costs of maintaining and operating the environment as new vulnerabilities are discovered.

With this in mind, and in collaboration with the VMware partner ecosystem, VMware has developed the Compliance Reference Architecture Framework (RAF), which allows organizations in regulated IT environments to automate and orchestrate technology and policy enabling more effective cyber risk management. VMware delivers regulation specific guidance, which includes validated compatible software and hardware solutions enabling a Compliant Capable, Audit Ready Platform.

For more information, please visit [VMware Compliance and Cyber Risk Solutions](#), where full compliance Reference Architecture documents for PCI, CJIS, FedRAMP and HIPAA are available. Please contact the Compliance and Cyber Risk Solutions team at [compliance-solutions@vmware.com](mailto:compliance-solutions@vmware.com) for details on the Compliance and Cyber Risk Solutions Program.

## Software Supply Chain Security

With global expansion of the software industry, security concerns have increased that a product or service could be compromised by malicious code introduced during product development or maintenance. Technological innovation and changes in sourcing and supply chain strategies have made software supply chain security a global challenge. Threats ranging from risks associated with using third-party code and open-source components to IP theft have dramatized the vulnerability of this new risk domain. VMware is actively engaging in proactive measures to minimize the occurrence of these risks and has launched several initiatives to address the security of our supply chain.

### Managing Supply Chain Risk

VMware utilizes a Supply Chain Risk Management program that focuses on secure sourcing of hardware, firmware, and software integration relating to building solutions. It includes use of an approved vendor list for several of its BUs and functions.

- VMware's recycle program for hardware products addresses supply chain risk by securely recycling equipment that may hold information sensitive to the supply chain. For example, hard drives that are at end of life and were used in the source control systems are properly recycled to ensure that the data from the source control systems is removed.
- VMware has established processes around partnerships with entities deemed to be of increased supply chain risk and around sharing source code with third parties.
- With respect to partnerships, VMware has an established process to determine if a partner is considered to be of increased security risk. Partners are carefully vetted prior to gaining access to programs.
- Both inbound and outbound contracts with software supply chain security implications are reviewed by Legal and Information Security teams. VMware includes terms that set minimum software security standards in its OEM (Original Equipment Manufacturer) and third-party software license agreements that are in keeping with or exceed industry best practices.



## Privacy

Building in appropriate security controls and safeguards in VMware products and services is integral to VMware's 'privacy by design' framework. The VMware security team and engineers work with the VMware privacy team during product development to evaluate security and privacy risks and implement safeguards to mitigate and minimize such risks and comply with applicable law. Further, as part of VMware's privacy program, VMware details the types of data collected in connection with its products and services in its [Products and Service Notice](#), and the types of data VMware collects and uses to manage accounts and customer relations in its [VMware Privacy Notice](#). The VMware Products and Services Notice contains information regarding the types of data collected and used in connection with VMware's provision of the Services.

## Security

As industry exploits attest, security cannot be bolted on just before a project is shipped--it must be an integral part of development from Day One. VMware builds our products with security from the ground up using leading security development tools, processes and methodology. VMware products are built on a comprehensive Security Development Lifecycle (SDL) methodology. Our VMware Security Response Center continuously monitors the security ecosystem and responds quickly to remediate vulnerabilities affecting our products and to mitigate risk for our customers.

## Product Security

VMware's Product Security team, internally known as the vSECR--VMware Security Engineering, Communication and Response--is responsible for protecting the VMware brand from a software security perspective. Its mission is to identify and mitigate security risk in VMware products and services. To achieve this, VMware has established oversight procedures that identify and mitigate potential product security risks throughout the development lifecycle. VMware has likewise instituted programs and practices that support both the development of secure products and solutions and drive security awareness across the enterprise. In response to risks to critical infrastructure, intellectual property, and sensitive information posed by the constantly evolving threat landscape, VMware has developed comprehensive and rigorous software security assurance processes and procedures that demonstrate the integrity of its products and address potential vulnerabilities.

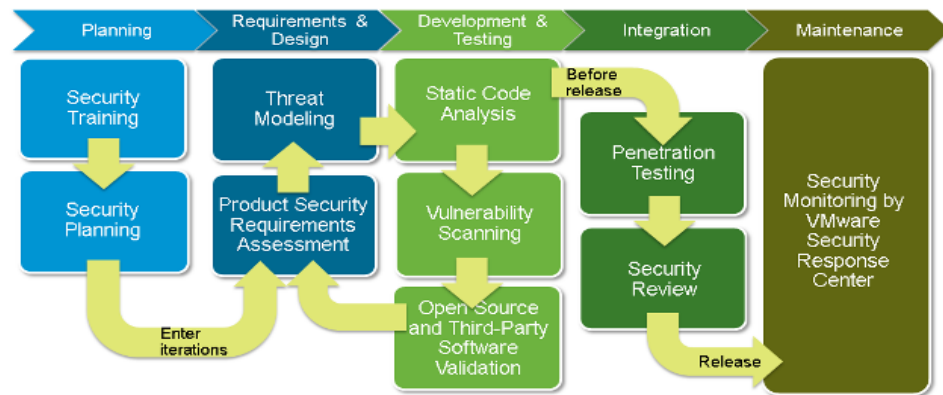
VMware is active in the broader software industry security community, becoming an early member of BSIMM (Building Security In Maturity Model) in 2009 and a member of SAFECode (Software Assurance Forum for Excellence in Code) in 2014, an organization driving security and integrity in software products and solutions. VMware is also active in the security research community and its Security Evangelism team works to actively cultivate relationships in this community. For example, VMware regularly brings speakers from the research community onto VMware campuses to present technical talks on security topics. VMware also hosts annual two-day internal security engineering conferences at multiple VMware facilities globally which include external security researchers and internal security experts from across the globe.

## Security Development Lifecycle

VMware's Security Development Lifecycle (SDL) program is designed to identify and mitigate security risk during the development phase of VMware software products. The vSECR group owns the definition and practice of SDL processes. It is continuously assessed for its effectiveness at identifying risk and new techniques are added to SDL activities as they are developed and mature.



## VMware Security Development Lifecycle



VMware Security Development Lifecycle

The SDL is the software development methodology promoted by vSECR to help VMware product development groups identify and mitigate security issues early in the lifecycle so that the development group's software is safe for release to customers. The SDL's end-to-end set of lifecycle processes aim to help product development groups achieve these goals:

- Reduce their component's risk profile and attack surface
- Identify and remediate costly security-related design flaws early in the development process before much coding has taken place.
- Discover and remediate security vulnerabilities prior to availability
- Educate their teams on security issues and security best practices

## Security Response Center (VSRC)

Established in 2008, VSRC is responsible for managing and resolving security vulnerabilities in VMware products once products are released to customers. VSRC has a mature process to investigate reports, coordinate disclosure activities with researchers and other vendors when appropriate, and communicate remediation to customers via security advisories, blog posts, and email notifications. VSRC is well established within the security research community and participates in many external security events in order to foster strong working relationships with the security research community. For example, VMware participates at major security conferences such as RSA, Black Hat, DEF CON, and CanSecWest, and is involved in the Bay Area security community. VMware's security response policies are well established and are publicly documented on the VMware website at

[http://www.vmware.com/support/policies/security\\_response.html](http://www.vmware.com/support/policies/security_response.html).

To learn more about the Security Development Lifecycle stages, the Security Response Center, Security Engineering, and Security Certifications, please see the VMware Product Security white paper at

<http://www.vmware.com/files/pdf/VMware-Product-Security.pdf>

## IT Information Security

The IT Information Security team maintains a formal, approved, resourced, and robust Information Security Program with the full support of the VMware executive leadership team which protects the Confidentiality, Integrity and Availability of any and all data within the VMware networks and systems.

Industry standard processes and controls are implemented and maintained in an up-to-date and secure manner. These fall into three main areas:



**Operational:**

- 24x7x365 live monitoring of security events and response
- Robust and thoroughly tested Computer Security Incident Response Team which has dedicated procedures for incident handling involving sensitive information and Breach Notification policies in accordance with applicable state, federal and international laws
- Stateful packet inspection firewalls with appropriate inbound and outbound rule sets
- Signature and anomaly based intrusion detection systems
- Application whitelisting controls on critical servers
- Operational intelligence monitoring for VMware, key partners and vendors and supply chain
- Centralized logging and monitoring with industry standard tools
- Regular patching of systems for security vulnerabilities
- Formal vulnerability management and penetration testing processes
- Whole disk encryption of key laptops and desktops
- Data Loss Prevention processes
- Periodic Third Party testing of the entire VMware infrastructure

**Architectural:**

- Design concepts such as Least Privilege, Separation of Duties, and Defense in Depth for Security Controls
- Separation of production and development environments with prohibitions on utilizing production data within development environments
- Multi-factor authentication for remote access

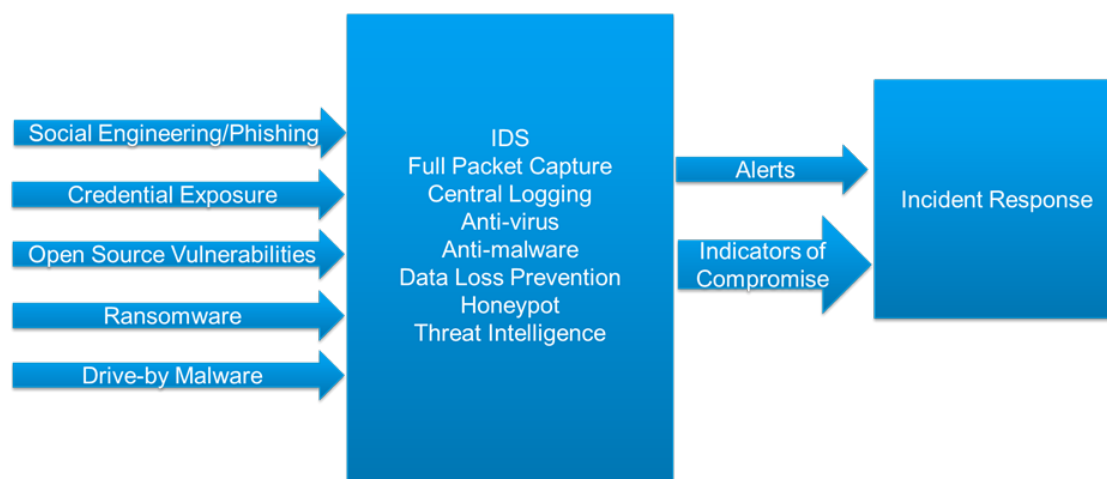
**GRC (Governance, Risk and Compliance):**

- Policies, procedures, and standards that are reviewed regularly and approved by senior management--such as the Data Classification Policy, Information Security Policy, Incident Response Policy, Remote Access Policy, and password policies requiring regular changing of passwords meeting complexity requirements
- Use of a Service Catalog approach to providing "Information Security as a Service" to the broader organization--definition and scope of each service offered, Service Level Agreements, and associated reporting and metrics
- Information security awareness training for key security topics through various delivery methods – videos, regular email notifications, and in-person events in VMware office locations
- Holistic assessments of risk across VMware and prioritization of risk mitigation efforts based on risk-ranking
- Overall governance of the Information Security Program utilizing a framework based on ISO 27001 principles and including appropriate components all the way from senior or executive management reporting (as well as the Audit Committee to the Board) down to operational metrics capture and dashboards
- Compliance controls design, monitoring and testing for key requirements such as Sarbanes-Oxley, HIPAA, PCI, and FedRamp

The following graphic illustrates VMware IT Information Security measures to address a variety of threats:



## Response: VMware Security “Stack”



## Commitment

VMware’s deep commitment to our customers’ success is well represented by strategically aligned teams that focus on addressing issues and enabling infrastructure. We draw upon many resources to help solve our customers’ challenges by providing a large, virtualization-specialized, Global Support Services (GSS) organization, and a growing ecosystem of certified solution and technology partners.

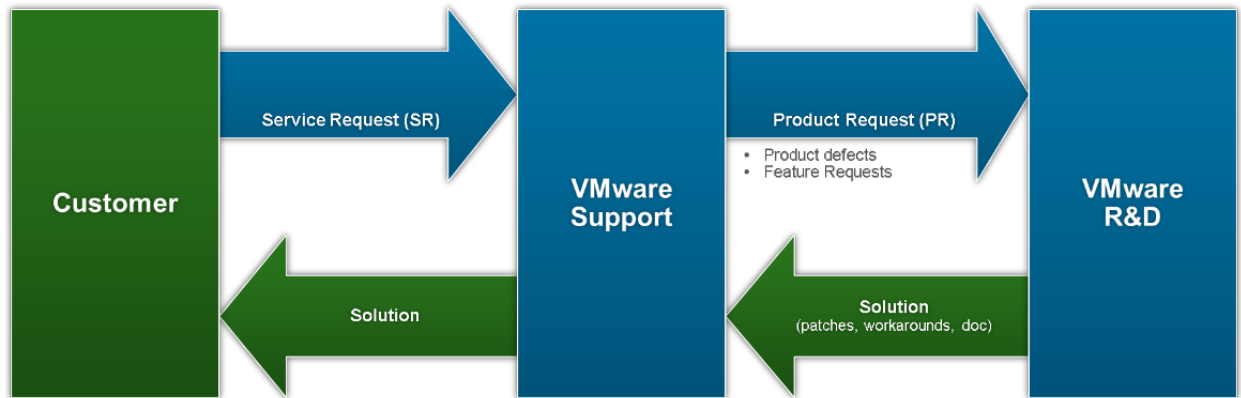
### Managing Critical Customer Issues

All development organizations provide escalation management along with the dedicated engineering focus to drive customer satisfaction and success through outstanding continuous product development. The following list of service offerings to customers is a value commitment.

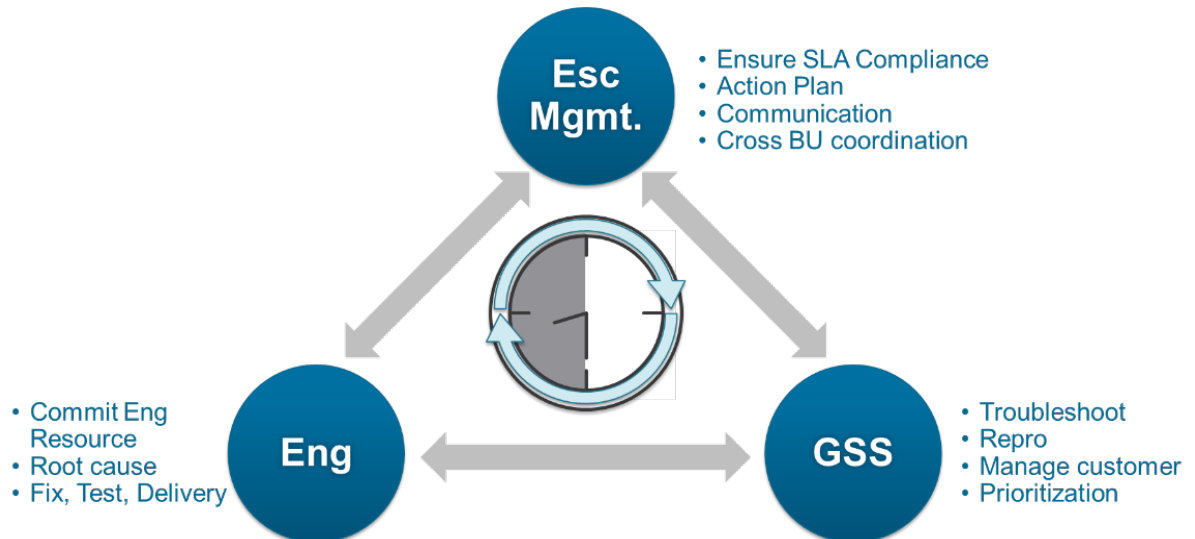
<b>Customer Management</b>	Escalation management
	GSS Interface
<b>Customer Engagement</b>	Service Request (SR) –Product Request (PR) handling, 24x7, SLA management
	Repro, Hot Patches
<b>Premier Support</b>	Repro, Hot Patches
	Align with GSS offering
<b>Maintenance Releases</b>	Payload: SR-PRs, Stabilization bugs, GOS Enablement
	Qualify and deliver maintenance releases
<b>Enhanced Maintenance</b>	Incremental product features, HW and SW enablement
	RPQ, Extended Support



The following graphic presents an end-to-end view of supporting customers, illustrating the engineering escalation process and engineering escalation execution:



Engineering Escalation Process



Escalation Execution

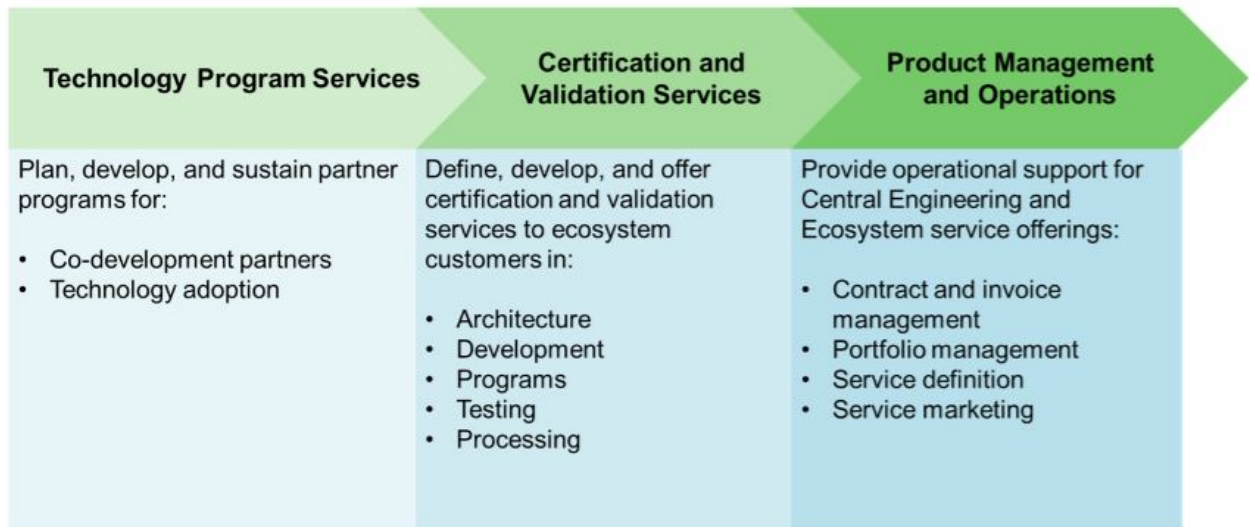
## Ecosystem Services

The VMware Ecosystem Services team's vision is to enable a healthy and growing ecosystem that provides a best-in-class cloud services experience for VMware customers. Their programs and practices bring strategic and essential value to our company-wide initiative of engendering customer trust in our products and solutions. This team offers over forty unique programs for over five hundred partner companies worldwide, resulting in more than twelve hundred TAP (Technical Alliance) partners with 13,000+ VMware Certified products.

The Ecosystem Services team's mission is to accelerate delivery and adoption of quality, compliant, and validated VMware products and services. This involves representing partners internally, VMware representation externally to partners, protecting and promoting the company brand, and optimizing the VMware ecosystem practices, processes, and tools through automation and simplification.



## Ecosystem Services



In partnering with the business units, the Ecosystem team's activities cover the full spectrum of support and collaboration. The technical facet of the program encompasses software--SDLC, product knowledge and access (pre-release), and technology enablement with scale.

Partner-facing activities include relationship management, expectation management, and roadmap alignment.

The business imperatives incorporate marketing, pricing and packaging, change management, and contract and legal.

Always critical, the team also oversees scaled communication, processes, and operations as applied to business flows (contracts, payment, support, utilization early access), project management (leadership, metrics), tools (DCPN, VCG, Developer Center, VMware Integration Validation (VIVa) etc.), and Certification.

The Ecosystem team's engagement with partners covers the entire spectrum of activities in the program life cycle:

### End to End Partner Ownership





## Customer Advocacy

### Why VMware Puts Customers First

Customers are core to VMware's "EPIC2" company values – the "C" stands for our Customers. At VMware, we seek to provide a world class customer experience from the inside out, which begins with a strong customer-centric culture. We aim to empower each employee with the insights, resources, and independence necessary to make choices that are in the best interests of both VMware and its customers. We strive to ensure that each employee understands his or her ability (and responsibility!) to impact the customer experience.

### Customer Advocacy

The Customer Advocacy team's focus is to represent the customer, partner and employee voice across the globe to champion a customer-centric culture. This team is laser-focused on the mission to ignite systemic business improvements across VMware that optimize the customer, partner and employee experience.

This team lives by a 'listen + act' philosophy: they deeply value customer input, are always listening, and are driving change based on what VMware customers tell them.

Insights from customers, partners, and employees enable this team to pinpoint strengths and, more importantly, translate those insights into concrete business actions. They seek to understand stakeholder's perspectives and perceptions of the VMware brand, services and solutions through a variety of formal and informal listening posts, including:

- **Live Conversations:** The Customer Advocacy team engages in direct conversations with VMware's customers and partners to better understand how to enable them.
- **The Inner Circle:** The Inner Circle is an online community of select customers & partners, to facilitate rapid cycle research efforts that shape VMware's priorities.
- **Surveys:** The customer, partner and employee voices are fundamental to building VMware's strategy and shaping company priorities. Survey programs enable VMware to consistently listen to stakeholders across the globe.

At VMware we listen, but more importantly we act. Customer Advocacy works directly with VMware's leadership to address improvement opportunities in the areas most critical to customers and partners. Based on recent feedback, we've focused on four key areas to take action:

- **Product Satisfaction:** Focusing on product consistency and functionality to satisfy customer needs
- **Strategy and Product Plans:** Increasing clarity and transparency around our company strategy and product plans
- **Engagement with VMware:** Enhancing sales and services engagements to ensure you get the most out of your VMware relationship
- **Partner Relationship:** Enabling VMware's partners to deliver the best possible solutions to customers

## VMware Global Support

VMware Global Support Services (GSS) is the world's largest virtualization support organization with fifteen years of experience supporting complex production and development environments. Working as a comprehensive unit, the team's mission is to provide outstanding levels of technical support using in-depth virtualization and cloud expertise. With support relationships with 100% of the Fortune 100, and 99% of Fortune 500 companies, this team delivers on aggressive resolution times and fast response times. GSS provides global coverage 24/7, 365 days/year, and follow-the-sun support for Severity 1 Issues. This large and important customer base underscores that VMware and our solutions have been widely trusted. It likewise reaffirms that our expert support organization is committed to maintaining and extending this trust into the future.



## Conclusion

Due to the ever-increasing complexity of modern infrastructure software, recent high-publicity component vulnerabilities, and high-profile data breaches and privacy concerns, there is a growing need for corporations to be more transparent about their products and processes in order to engender trust with their customers. VMware is meeting and anticipating these rapidly emerging threat trends and increasing customer transparency through the VMware Trust and Assurance framework, which aims at answering the most pressing customer concerns and showcasing why customers can rely on VMware to be their most trusted IT infrastructure vendor.

The programs and practices presented in this document have been designed to create high quality, secure products and solutions that VMware's customers can trust in the most critical operations of their enterprises. These initiatives have been tuned to advance and adapt to the frontline of our customers' evolving IT infrastructure needs, and attest to VMware's continuing commitment to our customers' success.



# Appendix

## Privacy Resources

- VMware Privacy Policy: <http://www.vmware.com/help/privacy.html>
- US-EU Safe Harbor List: <https://safeharbor.export.gov/companyinfo.aspx?id=22608>
- VMware Safe Harbor Notice: <http://www.vmware.com/safeharbor.html>

## Certifications

VMware has a long history of participating in FIPS and Common Criteria standards with the first VMware cryptographic module validated in 2007 and first VMware product being certified in 2008. The VMTA team drives the certification of major VMware products as well as the validation of cryptographic modules used in those and other products. The team also actively participates and contributes to the development of standards and various Protection Profiles by continuously engaging with various Working Groups (WGs)/NIAP Technical Committees (TCs)/International Technical Committees (ITCs).

For a complete list of VMware's Common Criteria certified products, visit

<http://www.vmware.com/security/certifications/common-criteria.html>

For a complete list of VMware's FIPS 140-2 validated modules, visit

<https://www.vmware.com/security/certifications/fips.html>

## More Information

For more information about VMware's product security programs and practices, see our Product Security white paper: <http://www.vmware.com/files/pdf/VMware-Product-Security.pdf>

Customer Advocacy website: <https://www.vmware.com/support/customer-advocacy.html>

VMware Trust and Assurance website: <http://vmware.com/trustvmware>





**VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 1-877-486-9273 Fax 650-427-5001 [www.vmware.com](http://www.vmware.com)**

Copyright © 2019 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.  
VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.





VMware, Inc.  
3401 Hillview Avenue (877) 486-9273 main vmware.com  
Palo Alto, CA 94304

November 9, 2021

To Whom It May Concern:

I attest that VMware Inc. has established the following Information Security policies for the purposes of protecting the integrity, confidentiality, and reliability of VMware information and information systems from unauthorized disclosure, removal, acquisition, modification or destruction:

Information Security Governance Policy  
Acceptable Use Policy  
Access Control Policy  
Asset Management Policy  
Authentication & Password Policy  
Back Up Policy  
Business Continuity Policy  
Change Management Policy  
Data Classification Policy  
End User Device Security Policy  
Encryption Policy  
Human Resources Information Security Policy  
Infrastructure Security Policy  
Logging & Monitoring Policy  
Operations Security Policy  
Physical Security Policy  
Production Control Policy  
Security Compliance Policy  
Security Incident Management Policy  
System Acquisition, Development & Maintenance Policy  
Third Party Risk Management Policy  
Vulnerability Management Policy  
Global Video Surveillance Policy

It should be noted that the VMware Security program and its associated Policies & Procedures are Proprietary and Confidential and therefore are not to be shared with outside entities. VMware information security policies were built in alignment with industry best practices / standards / frameworks such as NIST & ISO/IEC 27001, FIPS 140-2. Policies are reviewed on an annual and on an as-needed basis by the relevant stakeholders and revised as necessary. Policies are available for reference by all staff and contract resources and are hosted on the VMware Intranet.

Regards,

*Tim Mooney*

Tim Mooney  
Sr Director, Governance & IAM