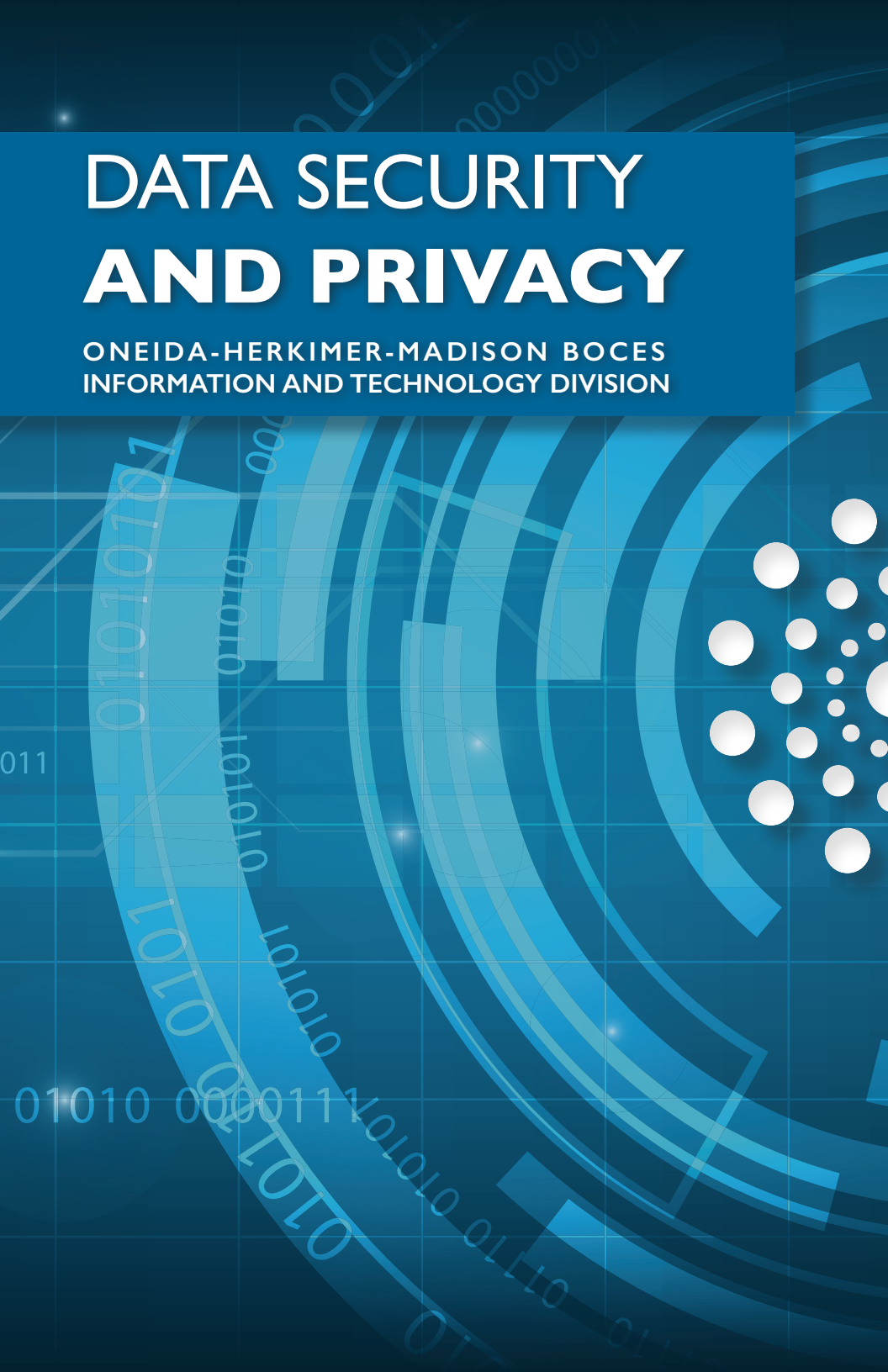

DATA SECURITY
AND PRIVACY
ONEIDA-HERKIMER-MADISON BOCES
INFORMATION AND TECHNOLOGY DIVISION

Data Security Practices

The increasingly connected, data-rich environments of today's schools, combined with readily-available exploitation tools, are causing districts to become more frequent targets of cyberattacks. These attacks can range from stealing or modifying data, holding information systems hostage, or simply causing disruption.

Regardless of the type of attack or the motive of the attacker, districts need to protect their information. Here are some relatively simple tips and best-practices to help guide districts through enhancing the security of their environments.

Personal, Private or Sensitive Information

Safeguard all sensitive information from unauthorized access, disclosure, modification and destruction to prevent access disruptions that could severely impact critical functions of a school district. Safeguard all sensitive district information, in addition to student information protected under NYS Education Law 2-d or FERPA.

Student Demographics
Student Grades
Student Discipline

Custody Information
Special Education Data
Health & Disability Information

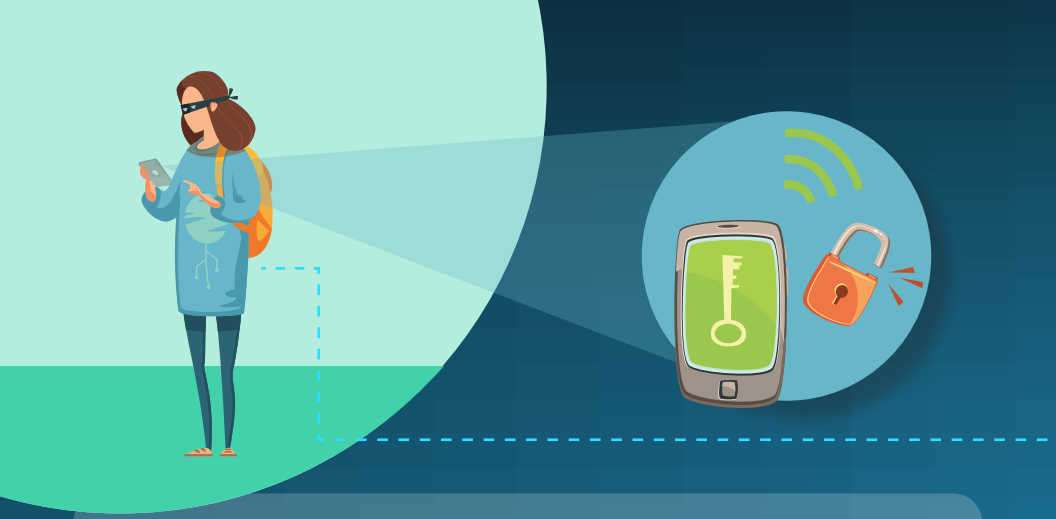
Financial Information
Teacher Ratings
Performance Evaluations

Information Security

Private and sensitive information contained within your district data systems should be treated with the utmost care. The data in these systems can be far more valuable to bad actors than banking or credit card numbers. Here are some quick data protection do's and don'ts:

- DO use system information only for the purpose directly related to performing your job duties or providing education.
- DO access sensitive information only from within secure environments through secure methods.
- DO lock workstations when leaving them unattended.
- DO ensure anti-virus and other security patches are up-to-date.

- DON'T utilize systems for personally identifiable or other sensitive information without reviewing the privacy policy and terms of use.
- DON'T share or discuss sensitive information with those who should not have access to it.
- DON'T leave passwords where others can see or easily find them.
- DON'T click links or download attachments from emails without verifying their authenticity.



Passwords

Passwords are your first and most important line of defense against system intrusion. They are essentially the keys to the kingdom and care should be taken to create and enforce appropriate policies. Here are some recommendations related to password security:

Strong Password Characteristics

- Minimum of eight characters, but the longer the better. Consider the use of a passphrase.
- Contains a mixture of character types (e.g. lowercase, uppercase, numbers, punctuation, special characters).
- Does not contain obvious keywords (e.g. 'password,' 'admin,' name of system, name of relative or pet).
- Does not contain common patterns (12345, qwerty, abc, aaaaa, 12321).

Password Handling

- Do not write down passwords. Refrain from storing passwords in easily accessible locations (e.g. sticky notes, under keyboards, unlocked drawers).
- Never share passwords with anyone.
- Always treat passwords as you would any strictly confidential information.
- Change account passwords in any system suspected of being compromised.

Administrative Practices

Quality policies, enforcement of policies and training of employees are all critical to effectively securing information. Here are some recommendations administrators should consider for their district:

1. Users should be trained at the time of their hiring and refreshed at least annually on laws, regulations, policies and best practices that should be followed to protect sensitive information.

2. Methods should be clearly defined and followed for granting access to and removing access from information systems.

3. The district should have an accurate inventory of all information systems utilized within the district, particularly those that house personally identifiable or other sensitive information.

4. Ensure technical measures are in place to protect data, including: anti-virus, software updates, internet filtering, firewalls, encryption, VPN access, etc.

5. Define procedures to efficiently respond to a data breach:

    - Notify all necessary parties.
    - Determine how the breach occurred.
    - Correct any altered data.
    - Take measures to prevent a reccurrence.

Avoiding Email Phishing Attacks

Phishing emails are one of the most common and effective methods cyber attackers will use to gain access to secure information.

- Check the "from" field to verify the sender.
- Hover over links within emails with your cursor to verify URLs.
- If you are unsure an email is authentic, verify with the sender.
- Think about the subject matter of an email and if it makes sense.
- Report suspicious email to your IT Department.

- Never send sensitive information through unencrypted email.
- Never open files attached to emails you do not recognize.
- Never click on links in emails without verifying the destination.
- Never click "Enable Macros" in unknown documents.
- Never respond or reply to spam in any way. Delete it.

Email — What to Watch For:

- From an Unrecognized Sender
- Please Click Link or Attachment
- Strange Subject Matter
- Bad Grammar or Spelling
- Offers and Deals
- Urgent or Threatening Requests
- Requests for Credentials
- Requests for Personal Information

Data Security Practices for Educators

Educational agencies are experiencing more frequent cyberattacks. These attacks involve stealing data, holding information systems hostage and causing disruptions in service. Follow these simple tips to help enhance your district's security.

Data Protection Reminders

Email Practices – Exercise caution before clicking on a link in an email or opening an attachment.

Workstation Practices – Lock workstations when leaving them unattended.

Password Practices – Establish strong passwords. Do not write down passwords and leave them in an easily accessible location.

Data Handling Practices – Use appropriate tools when handling data. Never send sensitive information through unencrypted email.

Privacy Practices – Do not establish accounts for students to access online resources without consulting with administration.

HUMAN BEHAVIOR IS AT THE ROOT OF 95% OF ALL CYBER SECURITY INCIDENTS.

Text adapted from:
RIC One "Data Security and Privacy" publication