Information Security Policy

1. **Purpose**

The purpose of this Information Security Policy is to establish guidelines and procedures to protect Poth ISD's information systems and data from unauthorized access, disclosure, alteration, and destruction. The policy aims to ensure the confidentiality, integrity, and availability of district information assets while complying with relevant legal, regulatory, and industry requirements.

2. **Scope**

This policy applies to all employees, students, contractors, volunteers, vendors, and any other individuals or entities who have access to Poth ISD's information systems, networks, and data.

3. **Roles and Responsibilities**

- Superintendent: Oversees the implementation and enforcement of this policy.
- Technology Director: Manages the security of information systems and infrastructure, ensuring compliance with this policy.
- All Employees and Users: Responsible for adhering to this policy and reporting any security incidents or concerns.

4. **Acceptable Use**

- District technology resources, including computers, networks, and email systems, are provided for educational and administrative purposes.
- Personal use of district technology should be limited and must not interfere with educational or administrative functions.

- Users must not engage in any activities that threaten the security of district systems, such as downloading unauthorized software, accessing inappropriate websites, or sharing passwords.

5. **Data Protection and Confidentiality**

- Sensitive student, employee, and district data must be protected following federal and state privacy laws such as the Family Educational Rights and Privacy Act (FERPA) and the Children's Internet Protection Act (CIPA).
- Users must follow established protocols for accessing, sharing, and storing sensitive information.
- All personal data must be encrypted when transmitted or stored on district systems.

6. **User Access Control**

- Access to district systems and data is granted on a need-to-know basis.
- Unique user credentials (usernames and passwords) are required for system access, and users must not share their login information with others.
- User access rights will be reviewed regularly, and accounts for individuals who no longer require access will be promptly deactivated.

7. **Network and System Security**

- Firewalls, anti-virus software, and other security measures must be used to protect district networks and systems from external threats.
- All software and systems must be updated regularly to address security vulnerabilities.
- Wireless networks must be secured, and access to guest networks must be isolated from district resources.

8. **Mobile and Remote Access**

- Employees and authorized personnel who access district systems remotely must use secure connections (e.g., VPN) and comply with district security protocols.
- Mobile devices that connect to district systems must be protected with passwords or biometric authentication.
- Lost or stolen devices must be reported immediately to the Technology Director for proper mitigation.

9. **Incident Response and Reporting**

- All users are required to report any security breaches or suspicious activities immediately to the Technology Director.
- A formal incident response plan will be implemented to investigate, contain, and mitigate the impact of security breaches.

- The district will comply with all legal and regulatory requirements for breach notification.

10. **Physical Security**

- Access to server rooms and other critical technology infrastructure is restricted to authorized personnel only.
- All workstations should be locked when unattended, and paper documents containing sensitive information must be stored in locked cabinets.

11. **Monitoring and Auditing**

- Poth ISD reserves the right to monitor network traffic, system access, and user activity to ensure compliance with this policy.
- Regular audits will be conducted to assess the effectiveness of security measures and to identify potential risks or vulnerabilities.

12. **Training and Awareness**

- All district employees and users will receive regular training on information security best practices and district policies.
- Users are responsible for understanding their role in protecting district information and reporting any potential security threats.

13. **Disciplinary Actions**

- Violations of this policy may result in disciplinary actions, including revocation of access to district systems, suspension, termination of employment, and/or legal action.

14. **Policy Review and Updates**

- This policy will be reviewed annually by the Technology Director and Superintendent to ensure that it remains relevant and effective in addressing emerging security threats and changes in technology.

15. **Compliance**

- This policy aligns with applicable state and federal laws, including FERPA, CIPA, and the Texas Education Code, and with district policies and procedures.

This policy outlines the key security practices to protect Poth ISD's data and information systems. All staff and users must understand and comply with these measures to ensure the safety of district assets.