



Cybersecurity Policy



Cybersecurity Policy for Fort Peck Community College

1. Purpose

This policy establishes guidelines to protect the confidentiality, integrity, and availability of the college's information systems, networks, and data. It ensures compliance with federal, state, and tribal regulations while respecting the unique cultural and educational mission of the college.

2. Scope

This policy applies to all students, faculty, staff, contractors, and third-party users who access the college's IT resources, including hardware, software, networks, and data storage.

3. Data Protection & Privacy

- a. All sensitive student, faculty, and institutional data must be securely stored and encrypted where applicable.
- b. Access to sensitive data is restricted to authorized personnel based on role-specific needs.
- c. Compliance with FERPA, HIPAA (if applicable), and relevant tribal data protection laws is mandatory.
- d. Personally Identifiable Information (PII) must not be shared without proper authorization.
- e. Regular data backups must be performed and securely stored both on-site and off-site.

4. Network Security

- a. The college shall implement firewalls, intrusion detection systems, and encryption protocols to secure network communications.
- b. All users must authenticate using secure login credentials, with multi-factor authentication (MFA) enforced where applicable.
- c. Unauthorized access, including hacking or network tampering, is strictly prohibited.



Cybersecurity Policy



d. Wireless access must be secured using strong encryption (e.g., WPA3) and segregated networks for guests and internal users.

e. Regular security audits and vulnerability assessments will be conducted to identify and mitigate risks.

5. Access Control

a. Access to college systems is granted based on the principle of least privilege (PoLP).

b. Employees and students must use college-provided accounts and are prohibited from sharing login credentials.

c. When an employee, student, or contractor leaves the college, their access must be revoked immediately.

d. Administrative privileges shall be restricted to essential personnel and subject to regular review.

e. Strong password policies, including complexity requirements and periodic changes, must be enforced.

6. Incident Response & Reporting

a. Any cybersecurity incident, such as a data breach or unauthorized access, must be reported immediately to the IT department.

b. The college will maintain an incident response plan that includes containment, investigation, notification, and mitigation steps.

c. Affected parties will be notified in accordance with legal and policy requirements.

d. The IT department will conduct a post-incident analysis to improve security measures.

7. User Responsibilities

a. All users are responsible for maintaining security by adhering to policies, reporting suspicious activity, and completing security awareness training.

b. Personal devices connected to the college's network must comply with security standards, including updated antivirus and operating systems.

c. Users must not install unauthorized software or disable security settings on college-owned devices.



Cybersecurity Policy



d. Phishing attempts, social engineering tactics, and other cybersecurity threats should be reported immediately.

8. Compliance & Enforcement

- a. Violation of this policy may result in disciplinary action, including loss of access privileges, suspension, termination, or legal action as applicable.
- b. The college reserves the right to audit and monitor IT systems to ensure compliance.
- c. Periodic cybersecurity training shall be mandatory for all students, faculty, and staff.
- d. This policy will be reviewed annually and updated as necessary to address evolving cybersecurity threats and compliance requirements.

9. Tribal Considerations & Sovereignty

- a. The cybersecurity policy respects tribal sovereignty and aligns with tribal governance and cultural considerations.
- b. Any collaboration with external cybersecurity agencies or vendors must comply with tribal laws and policies.
- c. Data ownership and management shall be governed by tribal regulations where applicable.

10. Policy Review & Updates

This policy will be reviewed annually by the IT department, in coordination with college leadership and tribal representatives, to ensure it remains current and effective.