ENFORCEMENT OF CYBERSECURITY REQUIREMENTS UNDER THE GRAMM-LEACH-BLILEY ACT (GBLA)

The Gramm-Leach-Bliley Act, signed into law on November 12, 1999, required financial institutions to implement certain information privacy protections and safeguards.

Five areas are frequently breached; they are:

- ☑ Data Mishandling – Separate duties, internal checklists
- ☑ Ransomware- Secure, test data backups on hand
- ☑ Stolen Credentials-multifactor authentication (MFA)
- ☑ Application vulnerabilities, Patches, and regular updates
- ☑ Phishing, annual training, CISA, NIST, recognize and report

The regulation requires a financial institution to disclose its policies and practices to protect the confidentiality, security, and integrity of nonpublic personal information about students/consumers. The Department of Education (ED) and Blackfeet Community College continue to take steps to ensure the confidentiality, security, and integrity of student and parent information related to the federal student aid programs. https://fsapartners.ed.gov/knowledge-center/topics/fsa-cybersecurity-announcements-and-guidance

STEPS TO IMPROVE DATA SECURITY:

1. **Backing up data and updating software:** Back up data regularly. If using an external storage device, keep it somewhere other than the primary workplace—encrypt it and lock it away if possible. Check backup files for accuracy. Ensure the backup isn't connected to a live data source so any malicious activity doesn't reach it. If you can update the system unit/computer, Select Start > Settings > Update & Security > Windows Update, then select Check for updates. If you cannot update the device, contact the IT Department for an update or patch.
2. **Strengthen your security with strong passwords and multi-factor authentication:** Using strong passwords on all devices and accounts where personal identifying information (PII) is stored is crucial. Protect passwords and login information from others and do not share them with other staff. These passwords should be complex, 12-15 characters long, hard to guess, and changed often. Never use the last five passwords. Using multi-factor authentication, a security measure ensures only authorized individuals can access PII data. It requires at least two separate forms of identification before granting access. For instance, you can use a password and a one-time code sent via text message. Password recommendations should include at least twelve characters, including numbers and special characters, and using an authenticator is highly recommended.
3. **Be aware of your surroundings:** Immediate surroundings are critical to campus data security. For example, while sitting in a meeting with a device or in a shared workspace, other people may be able to see the screen. Using privacy screens and other security measures is essential to maintaining vigilance. Suggestion: Use PII Masking when available. If you are working on a device, a privacy screen should be used outside the office, in meetings, or in other campus areas.

4. **Be wary of suspicious emails:** Know how to spot suspicious emails. Please be on the lookout for signs such as poor grammar, urgent requests, and payment requests. New technologies mean that email attacks are becoming more sophisticated. A phishing email may come from a recognized source. If you need clarification, speak to the sender by phone; do not click on suspicious links or links you do not recognize. The Federal Trade Commission has useful training materials to help recognize suspicious emails. https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams
5. **Install anti-virus and malware protection:** Ensure the devices employees use at home or when working away from the office are secure. Two-factor authentication would be the best way to remote access. Anti-virus software can help protect the device against malware sent through a phishing attack. BitLocker is highly recommended for portable devices with data from the BFCC student demographics.
6. **Protect your device when it's unattended:** Lock the device screen when leaving the office or to prevent others from accessing the computer. If you need to leave the portal device for much longer, lock the office door or place it in a secure, out-of-sight location, such as a locked cabinet or a desk drawer.
7. **Ensure your Wi-Fi connection is secure:** Using public Wi-Fi or an insecure connection could put personal data at risk. Always use a secure connection when you connect to the internet. Consider using a secure Virtual Private Network (VPN) if using a public network. Contact IT for the BFCC VPN, or let them know that we are working toward security and require a VPN.
8. **Limit access to those who need it:** Different workers may need to use different types of information. Put access controls in place to ensure people can only see the necessary information. For example, student accounts may need to see workers' personal information, but the maintenance staff won't. If someone leaves the company or is absent for an extended period, suspend their access to campus systems.
9. **Take care when sharing screen:** Sharing the screen in a virtual meeting may show others exactly what is on the desktop, including any open tabs or documents. Before sharing your screen in a virtual meeting, please close any unnecessary programs and ensure notifications and pop-up alerts are turned off.
10. **Don't keep data for longer than needed:** Get rid of no longer required data. Anything beyond three years on your computer should be deleted, not only to free up storage space. However, this also means that less personal information is at risk in the event of a cyberattack or personal data breach. Shred and delete all information as it is not needed for longer than the recommended three to four years.
11. **Dispose of old IT equipment and records securely.** Ensure no personal data is left on computers, laptops, smartphones, or any other devices before you dispose of them. Consider using deletion software or hiring a specialist or BFCC IT to wipe the data. Protecting that information is a shared obligation on campus, the departments, institutions, third-party servicers, and other partners in the financial aid system. There is an expectation to maintain strong security policies and adequate internal controls to prevent unauthorized access to or disclosure of sensitive information, including student and parent information. Contact the IT department for any information about the campus security software used. If you print paperwork, keep it in a locked file cabinet or locked file room, preferably fireproof, away from the office, and limit access to the Registrar, Admissions, and Financial Aid Directors. Other

access is on a need-to-know basis, or, if necessary, to file or work, access can only be granted by requesting the key from the director.

12. Who is responsible? The Student Aid Internet Gateway (SAIG) Agreement requires that postsecondary institutions (PSIs) report actual and suspected data breaches as a condition of continued participation in federal student aid programs. Data security affects everyone at PSI, from the president to applicants. No one is exempt from data security, and each person at the college plays a role in ensuring it. Title IV PSIs must report on the day that a data breach is detected or even suspected.

13. Reporting a breach: To report a breach, email cpssaig@ed.gov immediately. The email should include:

- date of the breach (known or suspected),
- impact of the breach (number of records, number of students, etc.),
- method of the breach (hack, accidental disclosure, etc.),
- those who are involved in the breach (names, department, etc.),
- information IT security program point of contact (email address and phone number are required),
- remediation status (complete, in-process, etc., with detail), and
- next steps (as needed).
- If you cannot email, call the Department's Security Operations Center (EDSOC) at 202-245-6550 to report the above data. EDSOC operates 24 hours a day, seven days per week.
- See Appendix D for the Cyber Security Incident Report Checklist in this manual.

14. How to send an encrypted attachment: Many applications can encrypt attachments: WinZip, Dropbox, DocuSign, Microsoft, etc. are some acceptable methods. The Federal Information Processing Standard (FIPS) is defined by FIPS 140-2. The minimum acceptable encryption is AES 256-bit for PSIs or separately encrypted attachments that are password-protected (with the password provided in a separate email).

- Tips to send an encrypted email message: click File > Properties. Click Security Settings, then select the "Encrypt message contents and attachments" checkbox. Compose an email message, and then click Send. Encrypt all outgoing messages. When encrypting all outgoing messages by default, write and send messages as you would with any other message. Still, all potential recipients must have your digital ID to decode or view your messages on the file tab. Choose Options >Trust Center > Trust Center Settings. On the Email Security tab, under Encrypted email, select the "Encrypt contents and attachments for outgoing messages" checkbox. Click Settings to change additional settings, such as choosing a specific certificate.

15. Faxing documents: When safeguarded, it is not a breach. It is assumed that a PSI has already performed a risk assessment and has secured access to the physical server. It is a further assumption that technical and logical controls are in place that would prevent individuals without a need to know (for example, system administrators) from viewing PII. More specifically, faxes arriving securely in a locked office when not in use would depend on how they arrive. If the fax is printed upon arrival from a fax machine, physical and administrative safeguards ensure the data is only viewed or handled by authorized personnel who need to know. Confidentiality and integrity are critical, whether in physical or digital environments.

16. Cyber security tools and techniques: What primary cyber security tools should be used? They are listed as:

2. Firewalls
3. Anti-Malware Software
4. Anti-Virus Software
5. Penetration Testing
6. Password Auditing and Packet Sniffers
7. Network Security Monitoring
8. Vulnerability Scanners
9. Network Intrusion Detection

17. FERPA Training for all staff at BFCC: Every year, the staff must retake the FERPA Training 101: For Colleges & Universities from the Department of Education. This online training course was developed by the Student Privacy Policy Office's Privacy Technical Assistance Center as an introduction to the Family Educational Rights and Privacy Act (FERPA) and its requirements relating to the privacy and security of Personally Identifiable Information (PII) in student records. This course addresses FERPA basics, explores the requirements for protecting student records for colleges, universities, and other postsecondary institutions, explains who may and may not access student records, when those records may be shared, and discusses several applicable exceptions to the FERPA requirement for consent. Once completed, the certificate is to be downloaded and submitted to their supervisor. The training can be found at **https://studentprivacy.ed.gov/training/ferpa-101-colleges-universities**