ABOUT THE GLB ACT

The Gramm-Leach-Bliley Act was enacted on November 12, 1999. In addition to reforming the services industry with respect to financial transactions, the Act addressed concerns relating to consumer financial privacy and data security. The Gramm-Leach-Bliley Act required the Federal Trade Commission (FTC) and other government agencies that regulate financial institutions to implement regulations to carry out the Act's financial privacy provisions (GLB Act). It required all covered businesses to take steps to protect customers' nonpublic personal information by July 1, 2001. Click on the link for more information about the Act on the FTC website.

GLB ACT REQUIREMENTS

The GLBA regulations include a Privacy Rule (16 CFR 313) and a Safeguards Rule (16 CFR 314), both of which are enforced by the FTC for higher education institutions. Colleges and universities are deemed to be in compliance with the GLBA Privacy Rule if they are in compliance with the Family Educational Rights and Privacy Act (FERPA).

- Privacy Rule
  The GLBA Financial Privacy Rule was created to regulate the collection and disclosure of nonpublic personal information between a financial institution and its customers.

- Safeguards Rule
  The Safeguards Rule requires institutions dealing in financial transactions falling under FTC jurisdiction to have necessary measures in place to keep customer information secure. The rule ensures that institutions develop, implement, and maintain a comprehensive information security program that contains administrative, technical, and physical safeguards that are appropriate to its size and complexity, the nature and scope of its activities, and the sensitivity of any customer information at issue. Such safeguards shall include measures that:
    - Ensure the security and confidentiality of customer records and information.
    - Protect against any anticipated threats or hazards to the security or integrity of such records; and
    - Protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

  Practical Tips for Safeguarding Customer Information:
    - Do not leave confidential data unattended or visible to others. Use password-activated screensavers.
    - Shred and never recycle documents containing confidential customer information.
    - Secure all daily work in locked file cabinets or drawers, and never loan your key/badge.
    - Talk quietly when discussing confidential or private information.
    - Sensitive information should not be sent to remote printers or faxes where access is uncontrolled and it should never be left on voicemail or answering machines.

UOTP SECURITY POLICY AND GUIDELINES FOR USING UOTP COMPUTERS

University-provided computers are subject to the same group policies as all computers on campuses. Per university policy, staff and faculty are the custodians responsible for all UOTP data on any university-provided computer they use. Their responsibilities are, but are not limited to:

- Protect university property stored on computers they use, including information about staff, faculty, students, and alumni.
- Access only that information which they are authorized to access in the course of their duties. Their ability to access other information does not imply any right to view, change, or share information.
- Do not establish access privileges for themselves or others outside of formal approval processes.
- Adhere to procedures and business rules governing access and changes to the data for which they are custodians.

The university expects all stewards and custodians of its administrative data to manage, access, and utilize this data in a manner that is consistent with the university's need for security and confidentiality. University of the Potomac administrative functional areas must develop and maintain clear and consistent procedures for access to university administrative data, as appropriate.

It is their responsibility to know what types of UOTP data they have on their computer and to take steps to protect it as outlined here and elsewhere in this security guide. At all times, staff and faculty must use the UOTP-provided laptop when working at home for reasons such as security, disaster recovery, and business continuity to ensure the protection necessary while working with institutional data.

Encrypt all confidential data
If staff and faculty have confidential data, or that comes home with them, that data must be encrypted. They must check with the IT department support staff to find out what encryption solutions are used.

Connect to campus with the Virtual Private Network
Connecting to UOTP's network from home increases the risk of data exposure or password compromises because staff and faculty have to use networks that are not controlled by the University. To minimize these risks, they should use the UOTP-provided laptop on which Virtual Private Network (VPN) software is installed when working with sensitive UOTP data. This will ensure that everything they do is encrypted as it goes over the network. VPN protects the data from electronic eavesdropping and may be required to connect to some department and central resources from off campus.

Secure home wireless network
Home wireless networks are easy to set up and extremely convenient to use. However, an insecure wireless environment poses several risks that need to be addressed:

- Anyone near the home can use the Internet connection.

- Anyone near the home may be able to access their computer.
- Anything sent over the wireless connection could be stolen.

The manuals that came with the wireless router should provide detailed information on how to secure the home wireless network. If they no longer have the manual, they can use the brand name and model type to search for an electronic copy online. Contact the University's IT department for further assistance.

Keep computers secure
At UOTP, staff and faculty ensure that all student information is protected and safeguarded from potential theft or data leaks. UOTP ensures that the level of data protection is not compromised and has enforced levels of security even when employees work from home. Staff and faculty must use only University-provided laptops and workstations.

Training
IT department provides training for every new software that staff members have to use as part of data security. All new staff members are trained in how to use the system and software provided by the university and are also updated on IT security policies by the IT department.

Security Measures for Software

Email G-Mail (G Suite)
- A notification is sent to the user as soon as the email account logs in to a new computer/laptop or is used to sign in using an app.
- Advanced Security Monitoring feature for G Suite users alerts administrators of any suspicious login if detected.
- The Advanced Security feature of G Suite also identifies phishing and potentially threatening emails (containing virus or malware) if a user receives them in their Inbox.

Salesforce
- Two-factor authentication is required if a user logs in to Salesforce from a new computer.

Student Information System (Sonis)
- Requires 2 login IDs and password authentication before a user can access the database.
- Geo-tag locking is in place so that the SIS system cannot be accessed from outside the US.

Employee laptops
- All University-provided employee laptops are set to Automatic download of Windows updates. The user is notified when the laptop needs to be restarted to install the updates.
- VPN software is installed on UOTP laptops/computers so that staff can access data saved on the university servers.
- Anti-Virus software is installed on all UOTP laptops to quarantine any potential/harmful viruses and malware when detected.
- Group Policies are set for domain-controlled computers which restrict installation of any additional software.

- Software such as Winrar and Adobe DC Pro are installed to password-protect documents and folders.
- Data storage and backup drive is available for all staff members using Google Drive, which comes along with the Gmail-hosted email accounts.

Faculty
All faculty members are instructed to use Google Meet to conduct classroom sessions. Google Meet is part of G Suite for Education and includes the security features mentioned in Google Workspace.

UOTP Server Infrastructure and Monitoring Policy

The University of the Potomac (UOTP) maintains a secure and reliable server infrastructure to support university operations, protect institutional data, and ensure business continuity.

Server Management
- University servers are maintained using supported Microsoft Windows Server operating systems and receive regular security patches and updates through Microsoft Windows Update and centralized IT management tools.
- Scheduled maintenance, including system updates, backups, testing, evaluation, and server restarts, is performed as necessary to maintain system performance, security, and reliability.

Endpoint Protection and Security
- All servers are protected with enterprise-grade endpoint security and antivirus software to detect and prevent viruses, malware, ransomware, and other cybersecurity threats.
- Multi-factor authentication (MFA), access controls, and security best practices are implemented where applicable to protect university systems and data.

Monitoring and Device Management
- The IT Department utilizes **NinjaOne** for real-time monitoring, endpoint management, alerting, software inventory, patch management, and remote administration of university-managed devices.
- **Microsoft Intune** is used to manage university-owned Windows devices, enforce security policies, deploy approved applications, and maintain device compliance.
- Security alerts, system health notifications, and critical infrastructure events are continuously monitored by the IT Department to ensure timely response to potential issues and consistent evaluation of the systems.

Data Backup and Disaster Recovery
- Critical university systems and data are backed up regularly according to the University's backup and disaster recovery procedures.
- Backup processes are periodically tested to help ensure data can be restored in the event of hardware failure, accidental deletion, or cybersecurity incidents.

Payment Security

- Online payment transactions are processed through secure, PCI-compliant third-party payment gateways.
- The University of the Potomac does not store, process, or retain payment card information on university servers.

Technical Support

- IT Help Desk support is available during normal university business hours by phone.
- Email support is available 24 hours a day, 7 days a week through **helpdesk@potomac.edu**. Requests submitted outside business hours are addressed according to the University's IT support and incident response procedures.

Student Records

The Office of Records and Registration maintains students' records. Student records include evidence of application and acceptance, admissions forms, official transcripts, registration records, financial records, and educational plans. Academic records, including grades and attendance, are generated electronically via the Learning Management System (Canvas) and integrated with the Student Information System (Sonis), which houses all academic records. Both cloud-based systems are password-protected with specific security permissions and undergo regular backups.

Maintenance of Records

University of the Potomac maintains a system of record retention in accordance with applicable federal and state requirements and consistent with accreditation standards and those of the American Association of Collegiate Registrars and Admissions Officers (AACRAO). It is the responsibility of the Registrar to establish and verify a system of record retention that is in accordance with federal and state requirements. Academic records are maintained for seven years after a student leaves school. Student transcripts are maintained indefinitely. In the event of a school closure, academic records are maintained by the Higher Education Licensure Commission (HELC) of the DC Office of the State Superintendent of Education, and the State Council of Higher Education for Virginia (SCHEV).

Privacy of Student Records

Policies and procedures concerning the privacy of student records are governed by the Family Education Rights and Privacy Act (FERPA) of 1974 (Public Law 93-380). Student records are maintained by the Office of Records and Registration. Students have the right to inspect and review their educational records, request amendment of their educational records, consent to disclosure of their educational records, and file a complaint with the US Department of Education.

Students aged 18 or over have access to their personal record files kept by University of the Potomac. All authorized Potomac personnel have access to student records for official purposes. A student (or in some cases an eligible parent) is given access to his/her record within a reasonable time after submitting a written request to the office in possession of the record. Students should allow 72 hours for a written request to be fulfilled. If the content of a record is

believed to be in error, inaccurate, discriminatory, or in violation of student rights or otherwise inappropriate, it may be challenged, and students may submit a written explanation to be included in the record.
Student information is released to persons, agencies, or legal authorities as required by subpoena/legal process or by consent of a student (or eligible parent). Information is released on a consent basis in cases where a student or eligible parent has provided written consent, signed, dated, and specifying the information to be released and the name(s) of persons to whom the information is to be released.

Directory Information
Colleges and universities may disclose, without consent, directory information. University of the Potomac designates the following items as directory information: Student name, address, telephone number, date and place of birth, major field of study, participation in officially recognized activities, dates of attendance, degrees, certificates, and awards received, e-mail address, and the most recent previous educational institution attended.

Right of Refusal to Provide Copies
University of the Potomac reserves the right to deny transcripts or copies of records not required to be made available under FERPA regulations. University of the Potomac designates the following items as directory information: Student name, address, telephone number, date and place of birth, major field of study, participation in officially recognized activities, dates of attendance, degrees, certificates, and awards received, e-mail address, and the most recent previous educational institution attended. If a student does not want any or all of the above information released, he/she should inform the Registrar's Office in writing by the fifth calendar day following the start of classes.

Risk Assessment

The University of the Potomac maintains a written risk assessment process designed to identify, evaluate, and manage reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, including student financial information and other nonpublic personal information protected under the Gramm-Leach-Bliley Act

Risk Assessment Process
The University's Information Security Program is based upon periodic risk assessments that:

- Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, destruction, or compromise of customer information.
- Evaluate risks associated with employee practices, information systems, third-party service providers, physical security measures, and business processes.
- Assess the adequacy and effectiveness of existing administrative, technical, and physical safeguards.
- Determine the likelihood and potential impact of identified threats and vulnerabilities.
- Document risk treatment decisions, including risk mitigation measures, risk acceptance decisions, and implementation priorities.

The Risk Assessment report is conducted annually. This report informs the Information Technology and Facilities Plan, and considers significant changes to information systems, business operations, and regulatory requirements.

Responsibility

The Qualified Individual is responsible for overseeing, implementing, and enforcing the University's Information Security Program and GLBA Safeguards Rule compliance. The Qualified Individual shall coordinate risk assessments, security monitoring, incident response procedures, and periodic reviews of the Information Security Program. The Qualified Individual manages the risk assessment process, ensures appropriate documentation is maintained, and recommends modifications based on evaluation results.

Program Review and Improvement

Information security safeguards are reviewed and adjusted as necessary based on:

- Risk assessment results;
- Security testing and monitoring activities;
- Changes in technology;
- Changes in business operations;
- Emerging threats and vulnerabilities; and
- Lessons learned from security incidents or near misses

Incident Response Procedures

Security incidents must be reported immediately. The Qualified Individual coordinates the response procedures, including investigations and documentation. Once appropriate corrective actions are taken, the results are incorporated into future risk assessments.

System Service Providers

The University follows the Vendor Management policy for selecting service providers. Vendors that create, receive, maintain, process, store, or transmit customer information on behalf of the University shall be subject to a risk-based security review prior to engagement. Contracts with applicable vendors shall require implementation of appropriate administrative, technical, and physical safeguards to protect customer information. The University shall periodically assess service providers to ensure continued compliance with contractual security requirements.

COMPUTER USE & ELECTRONIC COMMUNICATION POLICY

University of the Potomac (the "University") has established this policy with regard to the use of the University's computer equipment of all types, the network, and the telephone system (together the "system"). This policy covers the general use of the system, including all activity using the Internet and the use, access, and disclosure of electronic communications messages and images created, sent, or received using the system. Specifically, this policy covers all messages transmitted or received by telephone, voice mail, internal e-mail, and external e-mail, including chat rooms, and instant messaging.

In this policy "user" includes any student, employee, or guest of the University who uses or participates in the use of the system as it is defined above.

The college intends to enforce the policies set forth below and reserves the right to change them at any time as may be required under prevailing circumstances.

1. This policy is applicable at all times, which includes class time, work time, break time, after hours, and on weekends, and applies whether the user is on or off University premises during the use.
2. The system hardware is University property. All messages composed, sent, or received on the system are and remain the property of the University and are not the private property of any person.
3. The use of the system is reserved solely for the conduct of educational business activities at the University. It is not for personal use. All messages sent shall contain accurate identification of the sender.
4. The system may not be used for outside commercial ventures, religious or political causes, outside organizations, or other non-job related solicitations.
5. The system is not to be used to create, send, receive, or use any offensive or disruptive materials or messages. Messages which are considered offensive are those which contain sexual implications, racial slurs, gender-specific comments, or any other comment that offensively addresses someone’s age, sexual orientation, religious or political beliefs, national origin, or disability. Also considered offensive are messages which are fraudulent, harassing or obscene, and those which contain abusive, profane, or offensive language. Persons who wish to express personal opinions on the Internet must obtain their own user names on non-University owned systems.
6. The University reserves and intends to exercise the right to review, audit, intercept, access, and disclose all uses of the system. The contents of electronic officials without the permission of the author.
7. The confidentiality of any message should not be assumed. Even when a message is erased from the System, it is usually possible to retrieve that message. Further, the use of passwords for security does not guarantee confidentiality or privacy.
8. All users are responsible for seeing that the system and the Internet are separately and together used appropriately and in an effective, ethical, and lawful manner. The University has the right to determine what constitutes appropriate use of the System and

the Internet. Listed below are inappropriate uses of the system, the Internet, and University networks.

- Use for illegal activity or other non-school related purposes.
- Use for advertising, commercial and/or profitable purposes.
- Use to order or purchase any type of merchandise or services in the name of the University unless authorized, and/or any individual.
- Use for academic dishonesty.
- Use for political lobbying.
- Use for hate mail, discriminatory remarks, and/or use of copyrighted materials without permission of the copyright holder.
- Use to access or download obscene or pornographic material.
- Use to download and/or copy copyrighted music files without the express permission of the copyright holder.
- Use of inappropriate language and/or profanity.
- Use to transmit material offensive and/or objectionable to the recipient.
- Impersonation of another user and/or use of anonymity and pseudonyms.
- Loading, downloading, or use of unauthorized games, program files, or other electronic media.
- Destruction, modification, or abuse of networks, hardware, and/or software.
- Allowing an unauthorized person to use an assigned computer or account or revealing personal information, telephone
- numbers, addresses, etc. to other users of the networks.
- Unauthorized hacking, accessing, or circumventing security systems of any computer system, including University domains and network equipment.

9. Copyrighted material or trade secrets belonging to entities other than the University may be used only for legitimate and lawful purposes. Users are not permitted to copy, transfer, rename, add or delete information or programs belonging to others unless given express permission to do so by the owner. Failure to observe copyright or license agreements may result in disciplinary action from the University and legal action by the copyright owner.
10. To prevent computer viruses from being transmitted through the System, there will be no unauthorized downloading or loading of any software.
11. Users shall not use a code, access a communication file, or retrieve any stored communication information on the system unless authorized to do so. Users should not attempt to gain access to another person's messages without the latter's permission.
12. Any persons who discover a violation of this policy shall notify the Administrator of the system.
13. Any user who violates this policy or uses the System for improper purposes shall be subject to discipline, including discharge in the case of an employee, and probation or dismissal in the case of a student; and in all cases authorities may be notified.

14. A user shall be responsible for the cost incurred and damage to the System resulting from his or her negligent, willful, or deliberate acts, and for cost and damages from the use of the system in violation of this policy.