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 requires "financial institutions" to take steps to protect customers' nonpublic personal information. Click on the link for more information about the Act at the FTC website.

GLBA requirements

The GLBA regulations includes 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.

UOTP SECURITY POLICY

GUIDELINES USING UOTP COMPUTERS

The university provided staff computers are subject to the same group policies as all computers on campuses. Per university policy, you are the custodian responsible for all UOTP data on any university provided computer you use. Your responsibilities are and not limited to –

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

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 your responsibility to know what types of UOTP data you have on your computer at home and to take steps to protect it as outlined here and elsewhere in this security guide. At all times, 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 you have confidential data, or that comes home with you, that data must be encrypted. Check with your department’s IT support staff to find out what encryption solutions are used in your department.

Connect to campus with the Virtual Private Network

Connecting to UOTP's network from home increases the risk of data exposure or password compromise because you have to use networks that are not controlled by the University. To minimize these risks, you 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 you do is encrypted as it goes over the network. VPN protects your data from electronic eavesdropping and may be required to connect to some department and central resources from off campus.

Secure your 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 your home can use your Internet connection.
- Anyone near your home may be able to access your computer.
- Anything sent over the wireless connection could be stolen.

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

Keep your computer secure

At UOTP we ensure that all student information is protected and safeguarded from potential theft or data leaks. Today when most of us are working from home, UOTP ensures that the level of data protection is not compromised and have enforced levels of security even when employees work from home.

Avoid using personal computers/laptops for work related activities. Use only University provided 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 on how to use the system and software provided by the university and also updated on IT security policies by the IT department.

SECURITY MEASURES FOR SOFTWARE / PORTALS USED BY STAFF

Email G-Mail (GSuite)

- Notification is sent to user as soon as the email account logs in to a new computer / laptop or used to sign in using an app

– Advanced Security Monitoring feature for GSuite users alerts administrators of any suspicious login if detected

– The Advanced Security feature of GSuite also identifies phishing and potential threatening mails (containing virus or malware) if a user receives in their Inbox

SalesForce

– Two factor authentications is required if user logs in to Salesforce from a new computer

SONIS

– Requires 2 login IDs and Passwords authentication before user can access the database

– Geo tag locking is in place so that the SIS system cannot be accessed from outside US

Employee laptops –

All University provided employee laptops are set to Automatic download of Windows updates. 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 malwares when detected.

Group Policies are set for domain-controlled computers which restricts 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 Hangouts meet to conduct classroom sessions. The Hangouts meet software is part of the GSuite for Education and has security features as mentioned in the link below

https://support.google.com/a/answer/9822731

UOTP Servers

UOTP servers run on MS Server 2012 and is set to constantly run windows updates. Periodical backup and restarts are done to ensure everything is up to date.

Anti-Virus software is installed on the server to ensure that there is no virus or malware running on or the at backend of the server.

Spiceworks, a real – time monitoring tool is installed on the server for constant updates regarding the network and server warning of infiltrations, suspicious activity etc. The updates are constantly received by the IT administrator.

The online payment portal transactions are processed through a secured payment gateway and no card information are stored or saved by the university.

Help Desk support is available via phone during business hours and via email 24/7

helpdesk@potomac.edu

Privacy of Student Records

Policies and procedures concerning the privacy of student records are governed by the Family Education Rights and Privacy Act of 1974 (Public Law 93-380). Student records are maintained by the Registrar's Office (academic records), Financial Aid Office (financial aid records), and Student Finance Office (accounts receivable records). Files that are accessed by outside personnel are documented with date and the name of the person or entity accessing the file. Files are maintained in a locked room, in fire-resistant cabinets.

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.

SECURITY POLICY FOR STUDENTS

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 usernames 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.