

GALLAUDET UNIVERSITY
T1. Information Security Agreement (ISA)

As a user of Gallaudet University (GU) technology resources and data, I understand that I am responsible for the security of my User ID(s) and Password(s) to any GU computer system for which I am granted access. I understand that it is my responsibility to protect my password's confidentiality. I understand that I have the following responsibilities:

- Comply with Gallaudet University policies;
- Support compliance with federal and state statutory and regulatory requirements;
- Protect access accounts, privileges, and associated passwords (e.g., do not share passwords or login for others);
- Maintain the confidentiality of information to which I am given access privileges;
- Accept accountability for all activities associated with the use of my individual user accounts and related access privileges;
- Protect my computing devices, including
 - Do not disable or alter the anti-virus and/or firewall software;
 - Do not change the computer configuration, unless specifically authorized to do so;
- Use only licensed and authorized software;
- Ensure that my use of Gallaudet computers, technology devices, email, computer accounts, networks, and information accessed, stored or used on any of these systems is restricted to authorized duties or activities;
- Ensure the protection of my own personally-identifiable information (PII) and personal health information (PHI) when accessing self-service components of information systems;
- Unless there is an assigned or job-related duty, ensure that I do not access the records of any other person.
- Report all suspected security and/or policy violations via the Technology Help Desk;
- Report all known privacy and security violations to the Information Security Officer (ISO) and the Risk Management Director.

I understand that additional protections and responsibilities are expected where I have PRIVILEGED ACCESS (information beyond my own self-service data), system administrative duties, or access to information classified as CONFIDENTIAL or RESTRICTED in print, electronic, or signed/spoken form. Examples of CONFIDENTIAL data include personally-identifiable information, sensitive student information, financial records, social security and credit card numbers, protected health information, research data, and workforce (HR) records. Examples of RESTRICTED data include proprietary information, such as business plans, and other sensitive information. Dissemination of CONFIDENTIAL and RESTRICTED data is on a need-to-know basis.

I will sign a T1 System Access Request Form for all access beyond my own self-service data in enterprise information systems. I will comply with all Gallaudet University, Clerc Center policies and federal, state, and local laws and regulations concerning data access.

I understand that any CONFIDENTIAL and/or RESTRICTED information collected or obtained from, analyzed, or entered into any Gallaudet University information systems(s) or databases(s) is the property of Gallaudet University unless otherwise specified by contract. I will not access, use, and/or disclose CONFIDENTIAL and/or RESTRICTED information for any purpose other than the performance of authorized activities or duties. I will limit my access, use and disclosure to the minimum amount of information necessary to perform my authorized activity or duty (minimum necessary standard).

I will safeguard all CONFIDENTIAL and/or RESTRICTED information by holding it in the strictest confidence and by refusing to allow others to access information unless my authorized activities require that I do so. In such cases, I will disclose or allow access only to individuals having appropriate authority to access, receive, and use such information. In the cases where I have a conflict of interest or my duties would involve modifying the records of family members, I understand it is my responsibility to bring such information to my supervisor and to complete the [Conflict of Interest](#) form. I will avoid accessing or modifying any records where I might have a conflict of interest including records of family members. I understand that I may not exhibit or divulge the contents of any record or report to any person except in the conduct of my work assignment and in accordance with Gallaudet University policies and procedures. I will not acknowledge to anyone who is not a University official the existence of any student who has placed a confidentiality restriction on his or her information. I will not remove, copy, or print any official record or report, or copy thereof, from the office where it is maintained except in the performance of my duties and in accordance with established procedures. I understand that I am responsible for the protection of data that I access, query, or extract from University and Clerc Center data bases and will store or transmit such information only via secured devices and transport methods. If I have system admin duties, I understand that I am responsible for securing and encrypting data and data transmissions.

I understand that my access to systems may be monitored to assure appropriate access and compliance with system integrity. I understand that authorized use carries with it the responsibility to follow the Gallaudet University policies and procedures related to [uses of Information Technology resources](#). I understand that failure to comply with the above Information Security Agreement may result in disciplinary action. I have been given access to all of the Gallaudet University policies in the [Administration and Operations manual](#).

By signing this agreement, I understand and agree to abide by the conditions imposed above.

NAME OF WORKFORCE MEMBER	SIGNATURE	DATE
Title	Department	BISON ID



Note: If you don't know your BISON ID, you can look it up at <http://bison.gallaudet.edu>.

Click Self-Service > Personal Information Summary > Personal Information. BISON ID is on the top right side.

The following table is a glossary of terms used in the Information Security Agreement (ISA).

TERM	DEFINITION
Access	To view, use, or change information.
Authorized duties or activities	Duties or activities that are established by those with appropriate authority (e.g., division head, director, dean, chairperson, manager, or supervisor) related to the role or function of members of the workforce.
Authorized Software	Software that is authorized for use by the designated Data Stewards or Data Custodians.
CONFIDENTIAL Information	CONFIDENTIAL Information is information that is very sensitive in nature, and requires careful controls and protection. Unauthorized disclosure of this information could seriously and adversely impact Gallaudet University or the interests of students, other individuals and organizations associated with Gallaudet University. Examples include: personally identifiable information, protected health information, workforce records, student records, financial records, social security numbers, credit card numbers, legally protected University records, research data, and passwords.
Confidentiality	Expectation that information will be protected from unauthorized use or disclosure.
Disclose	Make known, reveal, release, transfer, or provide access to information in any manner.
Information Security Officer (ISO)	Gallaudet University has designated an Information Security Officer (ISO) who serves as the Privacy Official who assists in developing and implementing information security policies and procedures. The Privacy Official may identify or appoint designee(s) to assist in the performance of these functions.
Licensed software	Software that the Gallaudet University has been granted permission from the owner to use under a written license agreement or contract.
Minimum amount of information necessary	<p>Minimum Necessary Standard: When using or disclosing RESTRICTED or CONFIDENTIAL information, Gallaudet University must make reasonable efforts to limit disclosures to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. This standard does not apply to</p> <ul style="list-style-type: none"> • Uses and/or disclosures required by law or legal authorization • Uses and/or disclosures required for compliance with FERPA or HIPAA Privacy Regulations.
Personally identifiable information (PII)	<p>Personally identifiable information (PII) is information that is a subset of individual and student information, including demographic, financial, or sensitive information collected from an individual and:</p> <ul style="list-style-type: none"> • That identifies the individual; or • With respect to which there is a reasonable basis to believe the information can be used to identify the individual.
Privileged Access	Privileged access is access to information in Gallaudet systems and data bases that extends beyond one's access to one's own self-service data.
Protected health Information (PHI)	Protected health information is a subset of personally identifiable information maintained in permanent health records and/or other clinical documentation in either paper-based or electronic format.
Proprietary information	Gallaudet University possesses exclusive rights over the information within its systems. This includes business plans, financial information or other sensitive materials and information in printed, electronic or signed/spoken form that may affect employee rights or organization's operations.
RESTRICTED information	RESTRICTED Information is information that is business data, which is intended strictly for use by designated Gallaudet University employees and agents. This classification applies to information less sensitive than CONFIDENTIAL information. Dissemination of this information shall only be made to members of the Gallaudet University workforce or others with an established need-to-know.
Safeguard	Protect or cover from exposure, using precautionary measures.
System Administration Duties	System administration duties consist of all aspects of managing a technology-based information system, including but not limited to, user administration, front-office and back-office hardware and software configuration and management, data base administration, and network, domain, and other technology infrastructure management.
Workforce	Faculty, teachers, staff, students, temporary employees, contractors, interns and trainees, volunteers and other persons who perform work for Gallaudet University, and whose work conduct is under Gallaudet University direct control regardless of whether or not the workforce member is paid by Gallaudet University.