Protection and Use of Faculty, Staff, and Student Identifiers

Glossary

Confidentiality

Confidentiality is concerned with controlling the dissemination or publication of information that, if widely publicized, or obtained by unauthorized individuals, could result in harm to the subjects of the information. In some cases, certain types or classes of data are statutorily regulated and require data owners to implement certain controls to prevent the unauthorized disclosure of this information (see Regulated Data below).

Encryption

Encryption refers to the process whereby plain text is converted into humanly un-decipherable text by the application of an encryption algorithm. Encryption requires the use of a key that is applied to the plain text by the algorithm to generate the encrypted text. The same key is required to de-crypt the text in symmetric encryption. In asymmetric encryption schemes, a private-public key pair is used for the encryption-decryption process. Generally speaking, only the individuals who possess the key can read the encrypted text. Therefore, care must be taken to keep the keys secret to prevent unauthorized access.

Identifiers

For the purpose of this protocol, the term identifier applies to any data element that uniquely distinguishes any member of the University at Albany community. Different identifiers may be used for different business processes, and not all identifiers require the same level of confidentiality. The use and protection of some identifiers (e.g., Social Security numbers) are subject to statutory requirements (FERPA, NYS Information Security Breach and Notification Law, HIPAA). “Need-to-know” Because of the potential harm resulting from unauthorized disclosure, access to sensitive or regulated data should be governed and limited by the individual’s need to utilize that information for legitimate business purposes. As employees’ roles or duties change, so will their need to access different data collections and data elements (fields) within those collections.

Regulated Data

Regulated data refers to any data elements or data collections subject to regulatory controls. Examples of regulated data include education records (FERPA), personal health information (HIPAA), Social Security numbers (NYS ISBN Law, NYS Labor Law, NYS Public Officers Law), and financial records (FTC Red Flag Rules, Gramm Leach Bliley). Penalties for failing to comply with regulatory requirements can result in severe financial and operational sanctions (e.g., loss of federal education aid).

Security Domain

The University at Albany’s Information Security policy identifies ten domains which serve as a basis for protocol development and controls management. Examples of other domains include: Asset Classification, Access Control, and Incident Detection and Management.