Data Resource Summary
Appendix A

	Public	Limited Access	Restricted
Definitions	Data that has been approved by the BGSU Administration for public access.	Data BGSU may release if it chooses to waive exceptions to the public records law and place conditions or limitations on such release. Notification of unauthorized access is **not required** to the victims or other outside entities.	Data release prohibited by federal laws, state laws, and/or contractual obligations. For data to be defined as *restricted*, notification of unauthorized access is **required** to the victims or other outside entities.
Examples (This list has been created to provide examples and should not be considered as complete. It is the responsibility of each data owner to determine the classification.)	●Campus maps ●Department websites ●Course descriptions ●Course catalogs ●University/department brochures ●Press releases ●BGSU Directory Information *(unless non-disclosure has been requested by the student)* ●Enrollment statistics	●Intellectual property records produced or collected by BGSU faculty or staff. ●Research data not restricted by state or federal law or contractual obligation ●Internal memorandums not subject to Ohio public record laws. ●Proprietary information of BGSU ●BGSU ID numbers ●Campus security details	●Social Security numbers *(in combination with personally identifiable information)* ●Driver License number *(in combination with personally identifiable information)* ●Personally identifiable financial information ●Credit card numbers *(in combination with other data such as name, expiration date, security code etc)* ●Student education records ●Personally identifiable and protected health records ●Data prohibited from disclosure by contract or license agreement ●Human subject research data that identifies individuals.
Data Handling Guidelines	●None	● Should encrypt data on storage media ● Should encrypt data in transit ● Must limit access to authorized individuals ● Must report if information is exposed to their supervisor ● Must securely destroy past useful life ● Must only access, store, or modify on systems that are secure (examples include no viruses, password protected etc)	● Must encrypt data on storage media ● Must encrypt data in transit ● Must limit access to authorized individuals ● Must report if information is exposed to CIO ● Must securely destroy past useful life ● Must only access, store, or modify on systems that are secure (examples include no viruses, password protected etc)

**This chart is a summary of data classification and handling of data at BGSU. For more details on data classification and information on the appropriate data handling, please visit the Data Handling Guidelines and Data Classification Guidelines.*