Baldwin Wallace University Information Protection Quick Reference Guide

Area	Level 3: Restricted	Level 2: Confidential	Level 1: Internal	Level 0: Public	Implementation
Business Owner	Business owner must be identified for each type of information and define its classification level				* All information types are assigned a business owner; the information is classified appropriately; and communicated
Policy / Procedures	Policies and procedures must be in place and communicated to all associates regarding all information protection requirements; regular review process in place for updates as required; Ensure associate understanding through training and business support of requirements and enforcement				* Review & Update pertinent policies * Ensure policies are posted & communicated * Establish Governance periodic reviews (e.g. Audit)
Access Request	Data Governance Request Form Requires approval by the Data Owner AND one of the following: CIO, CISO or DPO	Data Governance Request Form Requires approval by the Data Owner AND one other member of the Data Governance Team	Data Governance Request Form Requires approval by the Data Owner only	Data Governance Request Form completed and reviewed by a Data Governance Team member	* Data Governance Request Forms are managed and reviewed by the Business Owner, or their designate, per the Data Classification Standard * Implement Identity and Access Management Solution - TBD
Access Review	User access must be reviewed by data owner quarterly with documented review	User access must be reviewed by data owner semi-annually with documented review	User access must be reviewed by data owner annually with documented review	N/A	* Access rights reviewed by the Business Owner or their designate * Implement Identity and Access Management Solution - TBD

Baldwin Wallace University Information Protection Quick Reference Guide

Area	Level 3: Restricted	Level 2: Confidential	Level 1: Internal	Level 0: Public	Implementation
Internal Sharing	Access restricted to authorized individuals by name (not groups) on a need-to-know or use basis; Must have the ability to have secure communications with internal associates for identified individuals		Access restricted to authorized groups or project teams on a need-to-know or use basis; Must have the ability to have secure communications with internal associates for identified groups	N/A	* Manually granting in IT Systems * Implement Identity and access Management Solution - TBD
External Sharing	Disclose to authorized business partners only on a need-to-know basis and with a signed non-disclosure agreement. Data Owner must approve; Must have the ability to have secure communications with external partners for identified individuals			Any public disclosure of information must comply with University Policy	* Information prtection requirements must be contained in the contract or disclosure agreement with external partner * Must comply with all policies
Storage	Information must be stored in secure location on the internal Baldwin Wallace University network or on an authorized external location with contract management in place; Information is required to be backed up regardless of location stored			Information on all Baldwin Wallace provided systems must be backed up	* Implemented through local IT procedures * Policy regarding Backup policy is in place * Enforced through correct access controls, Business Continuity, Diaster Recovery, and backup policies/procedures
Mobile	Baldwin Wallace University authorized Mobile Device Management (MDM) is required for mobile device access; Information must always be encrypted while at rest and in transit			N/A	* Implement MDM (Mobile Device Management) solution - TBD (Ex: InTune)

Baldwin Wallace University Information Protection Quick Reference Guide

Area	Level 3: Restricted	Level 2: Confidential	Level 1: Internal	Level 0: Public	Implementation
Copying / Printing	Proper printing procedures in place to ensure confidentiality of hard copy. Take reasonable precautions to restrict unauthorized access to copies by placing hard copy in locked containers. All printing activity sent to log management solution		Take reasonable precautions to restrict unauthorized access to information while printing and not leaving hardcopy in plain site unattended	N/A	* Use of a dedicated personal printer in an office * Use of person pin number to delay printout until user is at the printer * Hard copies locked in cabinets or draws
Records Retention	For each type of information; the legal and business requirement for its retention is defined; the business owner is documented; its disposal requirements are documented			N/A	* Implement a records management program for all data types
Disposal	Dispose in accordance with Baldwin Wallace University Record Retention Policy and the Data Destruction Procedures.			N/A	* Adhere to all university policies * Implement third party service for secure disposal of hardware * Non public hardcopy is shredded * Implement wipe software to clean hardware permanent memory such as hard drives being donated or returned on lease

Baldwin Wallace University Information Protection Quick Reference Guide

Area	Level 3: Restricted	Level 2: Confidential	Level 1: Internal	Level 0: Public	Implementation
Encryption (Internal & External)	Encryption solution required to protect information at rest and in transit		Encryption solution required to protect information in transit	N/A	* Implement encryption technology for data at rest (ex Azure RMS) * Implement whole disk encryption for all PCs (ex BitLocker) * Implement opportunistic TLS on all inbound and outbound email. * Use secure data transfer mechanisms such as sftp
Email	Always use Baldwin Wallace University approved email solution. Restrict auto-forwarding to non-company email. Do not send to recipient and email address you are not familiar with. Only send/forward to individuals authorized by information owner to access data.		Always use Baldwin Wallace University approved email solution. Restrict auto-forwarding to non-company email. Only send/forward to individuals authorized to access data.	Any public disclosure of information must comply with University Policy	* email configuration in place to stop auto-forwarding * Driven by current policy
Electronic File Transfer	Secure transmission required. Do not send to destination you are not familiar with. Only transmit to destinations authorized by information owner		Only transmit to destinations authorized by information owner	Any public disclosure of information must comply with University Policy	* Adhere to all university policies * sftp, https are examples, but standards/procedures vary by platform/app
Access Logging	Access logging must be turned on and logs sent to log management database		Access logging is at the discretion of the business owner.	N/A	*Log mgt required for Level 3 and Level 2 information

Baldwin Wallace University Information Protection Quick Reference Guide

Area	Level 3: Restricted	Level 2: Confidential	Level 1: Internal	Level 0: Public	Implementation
Monitoring / Management	Must have the ability to limit or detect content leaving the organization unprotected; Must be able to manage and monitor associates' ability to download data to personal devices and/or accounts; Must be able to manage/control associates' ability to share files with internal and external source			Any public disclosure of information must comply with University Policy	* Implement a Data Loss Prevention (DLP) solution * Adhere to all university policies * Implement a rights management solution (ex: Azure RMS) - TBD * Implement UEBA (User Entity Behavior Analytic) tool to monitor access restrict usage - TBD