

Quick Reference Guide: Data Classification and Handling

Data Classification	Examples	Where can I store this type of data?	Do not store	Disposal
<p>Restricted:</p> <p><i>This classification label applies to the most sensitive business information that is intended for use strictly within BSU. Its unauthorized disclosure could seriously and adversely impact the University, its customers (students), its business partners, and its suppliers.</i></p> <p>Marking: should be clearly marked as "Restricted"</p>	<ul style="list-style-type: none"> • Social Security Numbers • Credit Card Numbers • Banking account information • Passport Numbers • Driver's License Numbers • Health Insurance Portability and Accountability Act (HIPAA) Information 	<ul style="list-style-type: none"> • Encrypted Network File Share (X: Drive) • Secured File Cabinets/Desks 	<ul style="list-style-type: none"> • Portable devices (unless approved by DoIT) • Publicly available systems • Cloud storage (unless approved by DoIT) 	<ul style="list-style-type: none"> • Shred • Sanitize (please contact DoIT)
<p>Confidential:</p> <p><i>This classification label applies to less-sensitive business information that is intended for use within BSU. Its unauthorized disclosure could adversely impact BSU or its customers, suppliers, business partners, or employees. Information that some people would consider to be private is</i></p>	<ul style="list-style-type: none"> • Employee performance evaluations • Family Educational Rights and Privacy Act (FERPA) Information (e.g. student transcript data, student requests for data privacy) • Passwords • Internal audit reports. 	<ul style="list-style-type: none"> • Encrypted Network File Share (X: Drive) • BSU approved OneDrive or SharePoint Cloud File Storage System • Secured File Cabinets/Desks 	<ul style="list-style-type: none"> • Portable devices (unless approved by DoIT) • Publicly available systems • Cloud storage (unless approved by DoIT) 	<ul style="list-style-type: none"> • Shred • Sanitize (please contact DoIT)

Quick Reference Guide: Data Classification and Handling

<p><i>included in this classification.</i> Marking: should be clearly marked as "Confidential"</p>				
<p>Internal: <i>Information can be shared with BSU employees.</i> Marking: should be clearly marked as "Internal"</p>	<ul style="list-style-type: none"> • Employee Email • Departmental policies and procedures • Internal memos • Training materials • Research data not subject to specific confidentiality requirements 	<ul style="list-style-type: none"> • Encrypted Network File Share (X: Drive) • OneDrive • E-Mail System • External Storage Devices • On Top of Your Desk 	<ul style="list-style-type: none"> • Public systems • 	<ul style="list-style-type: none"> • Shred • Sanitize (please contact DoIT)
<p>Public: <i>Information can be shared with the general public.</i></p>	<ul style="list-style-type: none"> • Advertising and Marketing Materials • Public-Facing Web Sites 	<ul style="list-style-type: none"> • Unrestricted 	<ul style="list-style-type: none"> • Unrestricted 	<ul style="list-style-type: none"> • Unrestricted

Note: please follow the University's Data Retention Schedule to ensure you're not disposing of data that the University is required to keep for a specified time.