	Type	Description	Examples	Approved Storage Location
	Confidential (Category I)	This type includes: 1) University data protected specifically by federal or state law or Winston-Salem State University rules and regulations (e.g., HIPAA; FERPA; Sarbanes-Oxley, Gramm-Leach-Bliley; the North Carolina Identity Theft Statute; specific donor and employee data). 2) University data that are not otherwise protected by a known civil statute or regulation, but which must be protected due to contractual agreements requiring confidentiality, integrity, or availability considerations **Requirements when accessing, handling or storing:** - Only use university-supported cloud services, devices, or systems that have been approved by the university for handling confidential data. - Only share with personnel who are authorized to use it for legitimate business purpose; this includes verbal and written information. - Encrypt the data when sending or storing. - Ensure networks or systems used to handle or store the data have appropriate firewalls, monitoring, logging, patching, anti-malware, and related security controls. - Use university-provided systems or devices when accessing or processing data. - Contact the Information Security Office to ensure protection of data if compensating controls are used to secure the data in place of the above mentioned controls.	- Personal health information - Social security numbers - Credit card information - Driver's license numbers - Financial account numbers: including university account numbers, student account numbers, and faculty and staff direct deposit account numbers - Grievances/disciplinary action records - Court sealed records - Access control credentials - Non-Disclosure Agreements, Memoranda of Understanding, Service Level Agreements, Granting or Funding Agency Agreements, etc. - Student records - Crime victim information	**Cloud Storage:** - Microsoft OneDrive - Microsoft SharePoint **On-Campus File Server:** - Only department network drives **Removable Media Devices/Ext HDD:** - Not allowed - Exceptions must be approved by the Information Security Office before use
	Controlled (Category II)	This type includes University data not otherwise identified as Category-I data, but which are releasable in accordance with the North Carolina Public Records Statute (e.g., contents of specific e-mail, date of birth, salary, etc.) such data must be appropriately protected to ensure a controlled and lawful release. **Requirements when accessing, handling or storing:** - Only use university-supported cloud services, devices, or systems that have been approved by the university for handling controlled data. - Only share with personnel who are authorized to use it for legitimate business purpose; this includes verbal and written information. - Ensure networks or systems used to handle or store the data have appropriate firewalls, monitoring, logging, patching, anti-malware, and related security controls. - Use university-provided systems or devices when accessing or processing data.	- University and employee ID numbers - Employee date of birth - Employee email addresses - Donor information - Voicemail - Unpublished research - Contents of email - Fundraising data - Non-public contracts - Faculty and staff personnel records, benefits, performance apprasials, and employment applications	**Cloud Storage:** - Microsoft OneDrive - Microsoft SharePoint - Microsoft Teams - Adobe Creative Cloud **On-Campus File Server:** - Department & personal network drives **Removable Media Devices/Ext HDD:** - Not allowed - Exceptions must be approved by the Information Security Office before use

	Public (Category III)	This type includes University data not otherwise identified as Category-I or Category-II data (e.g., publicly available). Such data have no requirement for confidentiality, integrity, or availability. **Requirements when accessing, handling or storing:** - Data trustee allows access without authentication and data is made openly available	- Directory information - Public policies - Job postings - Service offerings - Published research - Degree prorgrams -	**Cloud Storage:** - Microsoft OneDrive - Microsoft SharePoint - Microsoft Teams - Adobe Creative Cloud **On-Campus File Server:** - Department & personal network drives **Removable Media Devices/Ext HDD:** - Not allowed - Exceptions must be approved by the Information Security Office before use **Public Access:** - Available for the public to access openly