



Policy number: 114
 Policy owner: Information Technology Services

Date of initial publication: June 6, 2017
 Date of latest revision: March 2, 2023

SCOPE

This policy applies to all staff, students, and contractors who handle data. It covers all data held by the University, regardless of whether it is stored on a physical or digital medium. The policy applies to all data, whether it is personal data, confidential data, or other sensitive data. The policy applies to all data, whether it is held on a physical or digital medium, and whether it is held on a server, a laptop, or a mobile device.

SCOPE AND AIMS

The aims of this policy are:

- Ensure that data is handled in a secure and appropriate manner.
- Ensure that data is protected from unauthorized access, disclosure, or loss.
- Ensure that data is stored and processed in a secure and appropriate manner.
- Ensure that data is disposed of in a secure and appropriate manner.

This policy applies to all data held by the University, regardless of whether it is stored on a physical or digital medium. The policy applies to all data, whether it is personal data, confidential data, or other sensitive data. The policy applies to all data, whether it is held on a physical or digital medium, and whether it is held on a server, a laptop, or a mobile device.

SCOPE

This policy applies to all staff, students, and contractors who handle data. It covers all data held by the University, regardless of whether it is stored on a physical or digital medium.

- **Data - A** (Confidential, Personal, Sensitive, etc.)
 This category of data is subject to the highest level of protection. It includes data that is confidential, personal, sensitive, or otherwise subject to legal or contractual obligations. This data must be stored and processed in a secure and appropriate manner, and must be disposed of in a secure and appropriate manner.
- **Data Owner** (Data Controller, Data Processor, etc.)
 The Data Owner is responsible for ensuring that data is handled in a secure and appropriate manner. The Data Owner must ensure that data is protected from unauthorized access, disclosure, or loss, and must ensure that data is stored and processed in a secure and appropriate manner.
- **Data Steward** (Data Controller, Data Processor, etc.)
 The Data Steward is responsible for ensuring that data is handled in a secure and appropriate manner. The Data Steward must ensure that data is protected from unauthorized access, disclosure, or loss, and must ensure that data is stored and processed in a secure and appropriate manner.
- **Data Custodian** (Data Controller, Data Processor, etc.)
 The Data Custodian is responsible for ensuring that data is handled in a secure and appropriate manner. The Data Custodian must ensure that data is protected from unauthorized access, disclosure, or loss, and must ensure that data is stored and processed in a secure and appropriate manner.

- FERPA- Protected Student Data - I
- Least Privilege Required -
- Personally Identifiable Information (PII) - A
- PCI-DSS – Payment Card Industry - D
- Protected Health Information (PHI) - I
HI AA

SC/DATA CAS

T I-G, II-, III-

T D D

I D I D E D

T D :

<p>Category IV. Red</p> <p>D T</p> <p>I</p> <p>A C I -</p> <p><u>M</u></p>	<p>E :</p> <ul style="list-style-type: none"> • C I (CI-D), C (C) C • H I (HI), I • I I (II)
--	--

Category I. Green

~~Category I. Green~~

E ~~Category I. Green~~

- G ~~Category I. Green~~



Appendix A to Data Security Classification Policy Data Category Epin

Date of initial publication: June 6, 2017
Date of latest revision: March 2, 2023

Faculty / Staff Information	Category Level
...T... E A	C... , I - G...
...A	C... , I - G...
...T... I	C... , I - G...
... I	C... , II - ...

()-E- (()0.)-13. (C)-7.)-8. ()- ()- ()7 8 8 8 8 8 8

