Standard: Electronic Transmission of Data Standard

Effective Date:	2017.06.23
Revision Date:	2020.02.06
Review Date:	2021.02.06
Approving Body:	Chief Information Officer
Authority:	Information Security Policy
Responsible Owner:	Director, Information Security and Compliance
Classification:	Public

Purpose

The Electronic Transmission of Data Standard describes the acceptable standards for electronically transmitting Protected and Restricted university information to protect the confidentiality and integrity of the data.

Who/what does the standard apply?

The requirements in this standard apply to electronic transmission of any Protected or Restricted University data. Transmission of data may be through email, automated data transfers between the university and external parties, or by other means. Data must be secured prior to transmission, during transmission, and after receipt. Acceptable protection methods include, but are not limited to:

- Password protected data transmitted via an email attachment
- Use of a Secure Channel for data transmitted between the University and External Parties
- Limiting access to data to those with the need to know
- Verifying External Parties meet the requirements of this standard

Definitions

- **Encryption:** is the conversion of data into a form, called a cipher text, which cannot be easily read by unauthorized people.
- **Restricted Data:** Information that is highly sensitive both externally and internally at the University. Unauthorized access could reasonably be expected to cause serious harm to individuals, businesses, other third parties or the University.
- **Protected Data:** Information that is sensitive externally and may be somewhat sensitive internally at the University. The inappropriate release of the Information would reasonably be expected to cause minimal to moderate harm to individuals, businesses, other third parties or the University.
- **Public Data:** Information that is intended for or is available to the public
- **Secure Channel:** transferring data with a set of security protocols that provide identity authentication and secure, private communication through Encryption, message validation and message authentication.

Compliance

Electronic data transmission must align to the requirements and specifications outlined within this standard. Where the electronic data transmission is unable to comply, please submit an Information Security Decision Request to the Director of Information Security and Compliance for review.

Specifications

Requirement	Specifications
Electronic data transmission must meet University requirements when transmitting Restricted or Protected data.	Data must be encrypted or protected with a password when transmitted outside of the University's private network.
Restricted or Protected data must be protected before and after the electronic data transmission.	Restricted or Protected University data must be encrypted when stored on a device. Access to Restricted or Protected University data must be limited to individuals who require access.
External Parties must meet the University's Electronic Data Transmission Standard.	Recipients of Restricted or Protected University data must maintain the Confidentiality and Integrity of the data they receive.

References

Policy, Procedure or Standard	
Information Security Policy and Procedure	
Data Security Classification Guideline	
Use of Computer Facilities Policy and Procedure	
Access and Privacy Policy and Procedure	