ROGER WILLIAMS UNIVERSITY
Information Security Policy

Purpose

Roger Williams University has created the following Information Security Policy in order to protect the confidentiality, integrity and availability of University Data as well as protect any information systems that store, process or transmit any University data. Roger Williams University finds it critical to protect all University information from accidental, malicious or unauthorized disclosure, misuse, modification, destruction, loss and/or damage.

Scope

This Policy applies to anyone who is authorized to access University data which includes but is not limited to: faculty, staff and third-party Agents of the University. Implementation of information security controls and Defense-in-Depth strategy allows the Information Security Team to identify and monitor security risks and create a stronger security environment for the University. These controls and strategy are to be reviewed and updated against industry best practices such as ISO and NIST.

Maintenance

This Policy is reviewed by Roger Williams University Information Security Office annually and on-going IT Security risk assessments are conducted regularly. All results and identified mitigation plans are shared with the Board Members via the Audit Committee.

Policy

Roger Williams University recognizes that in many instances it must collect, store and use sensitive information relating to its students, employees and individuals associated with the University. The Information Security Team is dedicated to collecting, handling, storing and using this sensitive information properly and securely. Throughout its lifecycle, all University Data shall be protected in a manner that is considered reasonable and appropriate.

RWU Information Security Governance

Roger Williams University requires that all users of the university computing infrastructure, devices or data comply with all applicable laws, regulations, statutes and university policies relating to information security and information technology. The University must be prepared to respond fairly and appropriately (1) to violations of law, regulation or university policy relating to information security, (2) when questionable or unacceptable computing practices occur, or (3) where there is non-compliance with information security policy requirements or with reasonable requests for action or cooperation necessary to implement the university's information security policies. Lack of compliance will result in sanctions or other appropriate action.