ELON UNVERSITY
Written Information Security Plan
Revised 12/2023

Contents

Revision Table

Effective Date	Author	Version	Approved	Change Reference
01/17/2019	Gary Sheehan	1.0	Christopher Waters	Initial Program Guide
06/05/2019	Gary Sheehan	1.0	Christopher Waters	Updated / added content
01/16/2020	Gary Sheehan	2.0	Christopher Waters	Replaced Internal Controls table
10/01/2021	Gary Sheehan	2.1	Christopher Waters	Fixed Formatting. Updated Metrics
12/13/2022	Gary Sheehan	3.1	Christopher Waters	Formatting / Legal Review
12/13/2023	Gary Sheehan	3.1	Christopher Waters	No Changes

Definitions

Availability: characteristic of the information by which it can be accessed by authorized persons when it is needed.

Confidentiality: characteristic of the information by which it is available only to authorized persons or systems.

Confidential Information: includes data and information regulated by state, federal or international laws, any data and information regulated by the Payment Card Industry and any Elon data and information that is not considered public.

Elon Assets:

- any equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information, including printers, storage devices, computers, computer equipment, network equipment and systems and phone equipment and systems.
- any software or technology system used to store, transmit, process, create or present information or data for university use
- any data or information used by Elon community members in the course of doing business for and on behalf of Elon University.

Elon Data: any information resource that is maintained in electronic or digital format. Data may be accessed, searched, or retrieved via electronic networks or other electronic data processing technologies.

Elon Senior Leadership: University President and members of Senior Staff

Information Security: preservation of confidentiality, integrity and availability of information.

Information Security Program: a segment of management processes that addresses the planning, implementation, maintenance, monitoring and improving information security within the University.

Integrity: characteristic of the information by which it is changed only by authorized persons or systems in an allowed way.

Overview

A Written Information Security Program (WISP) is designed to protect information and critical resources from a wide range of threats, to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities. Information Security is achieved by implementing a suitable set of controls, including policies, programs, processes, procedures, plans, technical controls and organizational structures (internal controls). These internal controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure the strategic and tactical business objectives of Elon University are met.

This program documents Elon University's (Elon) guiding principles, policies and best practices with respect to the protection of regulated, personal and University information and data subject to information security and compliance requirements. Elon has implemented this program, including the related administrative, technical, and physical safeguards appropriate to the nature and scope of its activities.

This program broadly addresses all aspects of maintaining a secure and compliant environment at Elon University as it relates to the protection of regulated information, sensitive University information and personally identifiable information. This program establishes and documents the administrative, technical and physical safeguards that are required to protect the technology, data and information assets of Elon University.

This program has been approved by the University Trustees and sets forth goals, objectives, policies, process and procedures for evaluating Elon University electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting regulated, personally identifiable information; Elon confidential information; and other University assets as described herein. This WISP in its most current version supersedes any prior policies, plans or requirements related to these topics. Elon's related policies and procedures will be reviewed by designated stakeholders at least annually for potential updates.

Purpose

Information security is critical to the interests of the University and the many constituencies it serves. This document identifies and documents specific standards, policies, procedures and processes to secure the confidentiality, availability, and integrity of our information technology infrastructure and certain protected data as set forth below. This document explains how and where the mechanisms have been implemented throughout the University and provides guidance for:

- Selecting appropriate security and compliance controls for information technology and information systems;
- Assessing Elon University internal controls;
- Determining security control effectiveness;
- Determining proper authorization of information systems;
- Monitoring and measuring the effectiveness of this Written Information Security Program;
- Ensuring the security, confidentiality, availability and integrity of Elon critical, regulated and personally identifiable information;
- Protecting against unauthorized access to, use or disclosure of such information ;
- Identifying, measuring and treating information security risks;
- Providing the foundation on which Elon University operates and safeguards its data and information systems to both reduce risk and minimize the effect of potential incidents;
- Ensuring compliance with industry requirements and international, state and federal laws that may require the university to take reasonable steps to protect the security of certain types of data, when applicable (e.g., FERPA, HIPPA, GLBA,GDPR, PCI, etc.)

Scope

This plan applies to any persons who access or use Elon Facilities or Assets, Confidential Information, Elon Data (the "Elon Community"), including faculty, staff, trustees, students, temporary employees, contractors, third-party service providers, business partners and alumni. In addition, this plan applies to all Elon University Assets, Confidential Information and Elon Data, whether the asset resides on campus or in the cloud.

In formulating and implementing this WISP, Elon University has agreed the following components are in scope for Elon University 's Information Security Program:

- All Elon University physical locations / facilities both on and off the main campus (each an "Elon Facility");
- All Elon University-owned or managed networks, network devices, computer systems, applications, or any other technology or computing assets ("Elon Assets");
- All Elon University proprietary or confidential information, including intellectual property ("Confidential Information");
- Any Elon owned or controlled individually identifiable personal data or other personal information for which the privacy, security, retention and confidentiality are regulated by applicable legal, regulatory and contractual requirements ("Elon Data");
- Elon Confidential Information and Elon Data stored at third-party locations.

Elon University is involved in every aspect of student living and education. As such, Elon University is subject to many regulatory and security standards and the following applicable standards having been identified as a priority for purposes of this WISP:

- Health Insurance Portability and Accountability Act ("HIPAA")
- Payment Card Industry Data Security Standard ("PCI-DSS")
- Family Educational Rights and Privacy Act ("FERPA")
- Gramm-Leach-Bliley Act ("GLBA")
- State of North Carolina laws regarding privacy, data breach and information security
- Title IX of the Education Amendments of 1972 (data retention)
- EU General Data Protection Regulation ("GDPR") and UK GDPR
- Other state privacy, security and data breach laws, as applicable

Further, Elon University has decided to base its required internal controls on the ISO 27002 Best Practices and Elon's business requirements. A list of those control areas can be found later in this document.

Information Security Strategic Plan

Strategy

Information Security will support the Elon University Strategic Plan, Finance and Administration's Strategic Plan and Information Technology's Strategic Plan and mitigate information technology-related risks and ensure compliance with legal, statutory, contractual, and internal University requirements.

Mission

The mission of Information Security is to enable the success of Elon University by mitigating risk and protecting and preserving information technology resources and Elon Assets, Confidential Information and Elon Data using the following guiding principles:

- To protect and preserve the confidentiality, availability and integrity of Elon University Assets, Confidential Information, and Elon Data and effectively manage potential risks.
- To enable the organization to meet its strategic goals and compliance requirements.
- To provide information security literacy and awareness to faculty, staff, students and university partners.
- To provide a safe and secure work environment for the Elon community.

Core Functions

To fulfil our mission and implement our strategy, Information Security will:

- Implement a proven security framework to establish and maintain a university-wide set of internal controls to mitigate risk, protect company assets and ensure compliance with applicable laws and regulations.
- Design and implement internal controls consisting of:
    - Policies
    - Standards
    - Processes
    - Practices
    - Procedures
    - Plans
    - Programs
    - Organizational structures

Internal controls will provide reasonable assurance that the University's objectives and strategic goals will be achieved, and undesired risk events will be minimized, prevented, detected and mitigated. Elon University will implement internal controls to ensure compliance and risk management by identifying, evaluating and managing information technology risk.

Information Security Program Responsibilities

Various leaders within the University have the primary responsibility and authority to ensure Elon University meets external and internal requirements for sharing, processing and storing Confidential Information, including intellectual property, research and institutional data, and Elon Data. Multiple departments are responsible for general security issues (legal issues, security compliance, physical security, communications, risk management, and IT infrastructure security). These individuals or departments are responsible for assisting in the development of university information security policies, standards, and best practices in their areas of responsibility. Specifically, the tables below outline Elon University's security responsibilities:

Information Security Program

Title	Purpose
Information Security Program Executive Sponsor	
Associate Vice President of Information Technology and Chief Information Officer (CIO)	• Overall responsibility for the management, operations and budgeting for Elon's information technologies and IT security. • Oversees the IT Risk Management Program.
Information Security Program Owner	
Director – Information Security	• Reports to the Chief Information Officer (CIO) and serves as an advisor on information security vision, strategy and direction. • Works collaboratively with the Elon Community to establish information security and IT risk management functions. • Responsible for Elon's Written Information Security Program and manages Elon's Information Security Awareness Program. • Coordinates the Elon IT Risk Management Program and advises university leadership on the identification and understanding of information and IT-related risks. • Oversees Elon's response to and reporting of information security incidents and provides guidance to incident investigations where appropriate.

Compliance Responsibilities

Role / Individual	Regulatory Responsibility
Associate Vice President for Student Life / Dean of Students / Assistant Professor **(Jana Lynn Patterson)**	HIPAA Compliance (Privacy and Security Rule)
Senior Business Analyst **(Tony Rose)**	Third-Party Services (Vendor/Supplier Management) – Contract Review
Associate Vice President for Finance and Administration **(Susan Kirkland)**	E-Commerce
Director – Information Security **(Gary Sheehan)**	PCI-DSS Compliance
University Registrar and Assistant Vice President **(Rodney Parks)**	FERPA Compliance
Director – Information Security **(Gary Sheehan)**	GDPR Compliance
Associate Vice President for Finance and Administration **(Susan Kirkland)**	GLBA Compliance

Information Security Operations (SecOps) Team

Team Member	Area of Responsibility
Christina Bonds	Enterprise Solutions
Alan Allred	Information Security Engineer
Robert Readling / Joel Bowman	Infrastructure / Network Security
Jeffrey Morton	CTS / Desktop / Laptop / Endpoint Security
Jerry Williams	Infrastructure / Network and Systems Security
Walt Garrison	CTS / Service Desk
Michael Shepherd	CTS / Apple /Mac IOS

Information Security Advisory Committee (ISAC)

(As of 2022, this group has been temporarily disbanded due to the inability of the committee members to meet on a regular basis)

Title	Purpose
Human Resources Information Systems Analyst	The Information Security Advisory Committee's purpose is to leverage the unique knowledge, experience and skills of individuals from outside the Information Technology department to address information security strategies, initiatives and tactical implementations. The Committee will monitor Elon's Information Security Program and make recommendations to Senior Leadership on enhancements to policy and internal controls. The Committee will promote visibility into the Information Security Program and increase awareness of its priorities among Elon Community Members. The Committee will achieve its purpose by providing non-binding advice to the Information Security Office in accomplishing the objectives of the Information Security Program, while maintaining alignment to the University's strategic goals. The Director of Information Security Officer will chair the Committee and will convene committee meetings on a quarterly basis, or as needed.
Admissions	
Faculty Rep	
Advancement	
Finance and Administration	
Assistant Director of Infrastructure / Engineer	
Assistant Dean of Student Development / Director of Student Involvement	
Assistant Registrar for Data Management and Reporting	
Director - Information Security	
Director of Global Engagement	

Information Security Document References

The table below lists the University documents either referenced in this Program document or impacted by information security internal controls, and thus are considered in-scope when information security changes are made, including documented information security policies, processes, standards and procedures.

Document Name	Document Type
Acceptable Usage	Policy
Access Control	Policy
Change Management	Standard
Computer Lab	Policy
Computer Lab Software	Standard
Department & New Employee Computer	Standard
Departmental Software	Standard
E-Commerce	Policy
Electronic Communication	Policy
Event Support	Policy
Firewall Security & Remote Access	Standard
Guest Account for Wireless Access	Standard
Information Security	Policy
MAC Address Restrictions	Standard
Maker Hub	Policy
Moodle Course Creation	Policy
Moodle Data Retention	Policy
Network Connection	Standard
Network Server	Standard
Password	Standard
Public Wireless Access	Standard
SSL Certificate	Standard
Supported & Non-Supported Information Based Technology	Standard
VPN	Standard
Web	Standard
Data Breach Response Plan	Plan
Problem Response Plan	Plan
Incident Response Plan	Plan
Written Information Security Plan	
Onboard / Offboard Account Procedures	Procedures
Account Change Procedures	Procedures

Information Security Internal Control Types

Internal controls can be either technical, physical or administrative and are classified as follows:

- Preventative controls exist to help prevent a potential threat from occurring.
- Detective / detection controls exist to help identify a potential threat.
- Corrective controls exist to mitigate or lessen the effects of the threat being manifested.
- Compensating controls may be considered when the University cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints but has sufficiently mitigated the risk associated with the requirement through implementation of other compensating controls.

For example, firewalls are primarily preventative controls. IPS could be configured to be both preventative and detective. IDS is purely detective. Re-imaging an operating system suspected of having malware is a corrective control. These are all examples of technical controls. Forensics and incident response plans are examples of administrative and/or technical corrective controls. Examples of compensatory controls include certain procedures like having a back-up generator, using a hot site for disaster recovery or physical asset isolation.

Information Classification

Elon University classifies data using the following criteria:

Sensitivity Level	Description
CONFIDENTIAL	The provision of access to CONFIDENTIAL DATA and INFORMATION must always align with Elon's Information Security and Access Control policies. Access to this type of information must be restricted to only those who have a legitimate business need. Sensitive information or Elon Data can only be shared when permission is given by the data owner. Elon Data includes the following, whether or recorded in any form or medium: A. All Elon Data, including demographic data or other personally identifiable information that permits identification of the individual or could reasonably be used to identify the individual or which is otherwise regulated by applicable privacy, breach and data security laws. B. Data or information that if breached, could have a major impact on the University and/or its reputation. Examples include Elon Data pertaining to personnel, faculty or students; key financial information; donor lists; proprietary information; protected health information regulated by HIPAA; credit card information; passwords and file encryption keys. C. Data or information which, if subject to unauthorized or improper disclosure, modification, or destruction, could trigger federal or state breach laws, result in civil or criminal penalties, or cause damage to Elon University or its reputation. D. Confidential information includes any proprietary business information, trade secrets, intellectual property or similar internal University information not publicly available. and which should be managed and secured to prevent unauthorized or public access.
PUBLIC	Public information is intended for use within Elon University and approved for public release. In some cases, this information can be shared with Elon business partners. This type of information is already, or can be, widely distributed within the University. Any information that is not explicitly classified as CONFIDENTIAL, can be distributed publicly.

Information Security Risk Management

Overview

Potential risk to an Elon Asset or Elon Data is determined based on the potential risk to the data, data subject, Elon asset and the University.

Many methodologies deal with risk management in an IT environment. Elon University's risk methodology focuses on 4 main areas, which include:

- Identifying and managing the risk to individuals and risk associated with productivity (a reduction in the ability of Elon University to effectively service its customers and community);
- Compliance (the cost of the overall legal procedure deriving from an adverse event);
- Competitive advantage (missed business opportunities due to a security incident); and
- Business reputation (missed opportunities or reduced enrollment due to the diminishing image following an event).

Purpose

Risk management is the process of identifying, analyzing and responding to risk factors in business processes and information technology. Proactive (rather than reactive) risk management will help reduce not only the likelihood of an event occurring, but also the magnitude of its potential impact.

Risk Management Methodology

Risk management is a critical component of Elon's Written Information Security Program. As such, Elon University monitors and manages potential risk to Confidential Information, Elon Data and Elon Assets through the execution of the following mechanisms:

- Annual Penetration Tests / Social Engineering Exercises
- Quarterly Vulnerability Scans
- Periodic Surveys
- Security Awareness Training
- Team Dynamix Ticketing System (to track Information Security Incidents)
- Implementation of Technical Internal Controls
- Implementation of Information Security Policies
- Compliance Reviews
- Vendor / Supplier Risk Management

Elon University 's Chief Information Officer oversees the Risk Management Program. Elon University 's Director of Information Security is responsible for reviewing and documenting all assessment findings, risk ratings, vulnerabilities and threats. Information security risk metrics are generated and shared with the appropriate levels of the University.

Risk Treatment

Effective risk treatment relies on attaining commitment from key University stakeholders and developing realistic objectives and timelines for implementation. The Director of Information Security will work with Elon University's Senior Leaders to choose security measures (if needed) to mitigate or reduce risk to an appropriate level. Risk treatment options include:

- **Avoiding the Risk** - terminating the activity that introduced the unacceptable risk, choosing an alternative more acceptable activity that meets business objectives or choosing an

alternative, lower risk approach or process.

- **Reducing the Level of Risk** - implementing an internal control that is designed to reduce the likelihood or consequence of the risk to an acceptable level.
- **Transferring the Risk** - implementing an internal control that transfers the risk to another party or parties, such as outsourcing the management of physical assets, developing contracts with service providers or insuring against the risk. The third-party accepting the risk should be aware of and agree to accept this obligation.
- **Accepting the Risk** - making an informed decision that the risk rating is at an acceptable level or that the cost of the treatment outweighs the benefit. This option may also be relevant in situations where a residual risk remains after other treatment options have been put in place. No further action is taken to treat the risk; however, on-going monitoring is implemented.

Vendor / Supplier Risk Assessment

Vendor Risk Management ("VRM") is the practice of evaluating business partners, suppliers, contractors and third-party vendors both before a business relationship is established and during the duration of a business contract. Third-party vendors and suppliers can expose their customers to potential risk. Elon's increasing reliance on third-party vendors, new privacy regulations, and shifting cybersecurity threats have impacted the third-party risk landscape. As a result, modern risk management solutions must address both internal risks, as well as the risk produced by doing business with partners, vendors, contractors, service providers and third-party suppliers.

To address this issue, Elon University performs a vendor assessment and thorough contract review before a contract is signed for a new service or product. Elon's Vendor Risk Assessment Team reviews the risk profile of each prospective vendor by:

- Reviewing contract terms
- Reviewing a completed vendor assessment survey

The team then rates the vendor and provides a recommendation to the Elon representative making the purchase. The Elon Vendor Risk Assessment Team consists of:

Team Member	Title
Christopher Waters	Associate Vice President of Information Technology and Chief Information Officer
Tony Rose	Senior Business Analyst
Gary Sheehan	Director, Information Security

Security Awareness & Training Program

Overview

Elon University is dedicated to protecting the organization's Confidential Information (including intellectual property), Elon Assets, and Elon Data. To help protect these interests, Elon University has implemented a security awareness and training program to educate our associates and third-party providers. This program is intended to set the training standards for all members of the Elon Community, including, but not limited to Elon University executives, employees and contractors. The success of the Elon University security awareness training program depends on the ability of all users to work toward a common goal of protecting the organization's sensitive, critical, and regulated information and data.

All Elon employees are required to take annual Security Awareness Training.

Scope

This program impacts all Elon Community members and is intended to help users be aware of actions they can take to better protect the organization's information as well as their personal information.

Awareness / Training Requirements

All Elon community members are required to participate in the following activities:

- Attend annual awareness training (mechanism for delivery to be determined each calendar year). Training may vary year-to-year based on current trends. Failure to complete the annual training may result in disciplinary actions. Training awareness mechanisms can include video training, Lunch-n-Learn Sessions, Department Meetings, College Coffee Sessions, New Hire Orientation and other University-led training opportunities.
- Read the periodic briefs, insights, instructions and updates circulated by Information Security with the intent to inform and educate individuals.
- Attending onboarding security awareness training and education. New employees may be denied access to Elon University systems until such requirements have been met.

Internal Controls (Policies / Procedures / Technologies)

The table below lists the set of internal controls (best practices) documented in ISO 27002:2022. These controls identify the policies, processes, plans, programs, procedures, technologies and organizational structures that Elon University maintains to help manage risk, comply with regulations and secure Elon University ’s information technology environment.

The controls listed in this table are reviewed annually and used to calculate Elon’s level of potential risk exposure.

Internal Control	Description
Information security policies / Plans / Processes and Procedures exist and have been communicated appropriately.	A set of policies for information security are defined, approved by management, published and communicated to employees and relevant external parties.
Review of the policies for information security.	The policies for information security are reviewed at planned intervals (at least annually) or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.
Leadership Support	Senior Leaders ensure adequate resources are available to support Elon's information security requirements.
	Senior Leaders demonstrate leadership and commitment to information security and risk management.
	Senior Leaders encourage all Elon Community members to practice security in accordance with established policies and procedures of the University.
Information Security Roles and responsibilities	Adequate information security resources have been assigned to specific security roles and responsibilities.
	Information security roles and responsibilities are documented.
Segregation of duties	Conflicting duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the University’s digital assets, including Elon Data.

Internal Control	Description
Employment Screening	Background verification checks on all candidates for employment are carried out in accordance with relevant laws, regulations and ethics and proportional to the business requirements, the classification of the information to be accessed and the perceived risks.
Terms and conditions of employment	Employees agree to and sign the terms and conditions of their employment contract.
Information security awareness, education and training	The University's workforce receives initial security awareness training upon being hired.
	The University's workforce receives appropriate and periodic security awareness training and education as relevant for their job function.
Disciplinary process	There is a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.
Termination or change of employment responsibilities	Information security responsibilities and duties that remain valid after termination or change of employment are defined and communicated to the employee or external party user and enforced.
Inventory of assets	Assets associated with information and information technology are identified and an inventory of these assets are drawn up and maintained.
	Assets maintained in the inventory have a designated owner.
Return of assets	All employees and external party users return all the University assets in their possession upon termination of their employment, contract or agreement.
Classification of information	Information assets are classified in terms of risk, value, legal requirements, sensitivity or criticality to the University.

Internal Control	Description
Management of removable media	Procedures are implemented for the management of removable media in accordance with the classification scheme adopted by the University.
Disposal of media	Formal procedures have been implemented and are followed when sensitive media is disposed.
Physical media transfer	Media containing sensitive information or Elon Data are protected against unauthorized access, misuse or corruption during transportation.
Identity and Access Management	Users only have access to the network and network services that they have been specifically authorized to use.
	A formal user access provisioning process is implemented and documented to assign or revoke access rights for all types of user, system and service accounts.
	The allocation and use of privileged access rights are restricted and controlled and periodically inventoried.
	The access rights of all employees and external party users to information and information processing facilities are removed upon termination of their employment, contract or agreement, or adjusted upon change.
Information access restriction	Access to information and application system functions are restricted in accordance with the access control policy.
Password management system	Password management mechanisms are interactive and ensure quality passwords and meet University requirements.
Encryption	Encryption is used to protect regulated and sensitive data both at rest and in transit and according to international, federal and state regulations.

Internal Control	Description
Physical entry controls	Secure areas such as data centers and equipment closets are protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
Equipment siting and protection	Equipment is positioned and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
Supporting utilities	Equipment is protected from power failures and other disruptions caused by failures in supporting utilities.
Equipment maintenance	Equipment is correctly maintained to ensure its continued availability and integrity.
Security of equipment and assets off-premises	Security is applied to off-site assets considering the different risks of working outside the University's premises.
Secure disposal or re-use of equipment	All items of equipment containing storage media are verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.
Unattended user equipment	Users ensure that unattended equipment has appropriate protection.
Documented operating procedures	Information security operating procedures are documented and made available to all users who need them.
Change management	Changes to the University's business processes, information and information technology systems are controlled.
Separation of development, testing and operational environments	Development, testing, and operational environments are separated to reduce the risks of unauthorized access or changes to the operational environment.
Controls against malware	Detection, prevention and recovery controls to protect against malware are implemented.

Internal Control	Description
Information backup	Backup copies of information, software and system images are taken and tested regularly in accordance with the agreed backup policy.
Event logging	System event logs are produced, stored, protected and regularly reviewed.
Administrator and operator logs	System administrator and system operator activities are logged, protected and regularly reviewed.
Management of technical vulnerabilities	Information about technical vulnerabilities of information systems is obtained in a timely fashion to determine the University's exposure to such vulnerabilities and appropriate measures taken to address the associated risk.
Network controls	Networks are managed and controlled to protect information at rest and in transit.
Segregation in networks	Groups of information services, users and information systems are segregated on networks where required.
Agreements (Contracts) on information transfer	Agreements address the secure transfer of business information between the University and external parties.
Electronic messaging	Information involved in electronic messaging is appropriately protected.
Security requirements analysis and specifications	The requirements for information security controls are included in the statements of business and technical requirements for new information systems or enhancements to existing information systems.
Securing application services on public networks	Information involved in application services passing over public networks are protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.

Internal Control	Description
Protecting application services transactions	Information involved in application service transactions is protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.
System change control procedures	The implementation of changes is controlled using formal change control procedures.
Technical review of applications after operating platform changes	When operating platforms are changed, business critical applications are reviewed and tested to ensure there is no adverse impact on university operations or security.
Secure development environment	The University has established a secure development environment for system development and integration efforts that covers the entire system development lifecycle.
System security testing	Tests of the security functionality are carried out during development.
System acceptance testing	Acceptance testing programs and related criteria are established for new information systems, upgrades and new versions.
Addressing security within supplier agreements	All relevant information security requirements are established and agreed with each supplier that may have access to, process, store, communicate or provide IT infrastructure components for the University's information.
Incident Response	Management's responsibilities and procedures are established to ensure a quick, effective and orderly response to information security incidents.
	Information security events are reported through appropriate channels as quickly as possible.
	Information security incidents are responded to in accordance with the documented procedures.

Internal Control	Description
	Knowledge gained from analyzing and resolving information security incidents are used to reduce the likelihood or impact of future incidents.
Disaster Recovery / Business Continuity Planning	The University has established, documented and periodically tested a disaster recovery plan for IT assets and technologies.
	The University has verified their Disaster Recovery Plan adequately supports their Business Continuity Plan.
Identification of applicable legislation and contractual requirements	All relevant statutory, regulatory, contractual requirements and the University's approach to meet these requirements are explicitly identified, documented and kept up to date for each information system and the University.
Intellectual property rights	Appropriate procedures are implemented to ensure compliance with legislative, regulatory and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.
Protection of records (PCI, FERPA, GLBA, HIPAA, GDPR, etc.)	Records/Data/Information are protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with statutory, regulatory, contractual and business requirements.
Independent review of information security	The University's approach to managing information security is ongoing and its implementation is reviewed independently at planned intervals or when significant changes to the security implementation occur.
Technical compliance review	Information systems are regularly inspected for compliance with the University's information security policies and standards.

Metrics

Elon University needs to monitor its information security metrics and communicate the results to senior leadership and trustees, so they can understand the potential risk exposures Elon faces as they strive to meet their strategic goals. Metrics also help confirm the tactical solutions deployed to mitigate security exposures and unacceptable risk are operating as expected. Lastly, metrics help the CIO and Director of Information Security determine if the Written Information Security Program is effective and efficient. To achieve these goals, the Information Security Team will collect data to report the following metrics:

> **OBJECTIVE:** To identify, measure and manage potential risks to the confidentiality, integrity, availability and privacy of Elon's Assets, Confidential Information, and Elon Data and the technology used to access, process, store and transmit such information assets.

The figure below represents the metrics being recorded for the 2023-2024 academic year.

Information Security Metrics																		
Month	REPORTED SECURITY INCIDENTS (Tickets)						InfoSec Training Participants (Completed YTD)	TECHINCAL RISK METRICS			Human Risk	Vendor Risk Management	VULNERABILITY SCANS - RISK SCORES					Monthly IT Risk Score
	# of Comp'ed Accts	Lost / Stolen Dervice	InfoSec Problem Tickets	Total Number of InfoSec Tickets	Open Vulnerability Management Tickets	Open Sec. Tickets		DNS Requests Blocked	Cyber Risk Score	IT Internal Risk Score			Systems	ERP	CTS	Network	Apps	
June	6	0	2	322	71	0		1,114,995	100	100		70	15	30	16	20	1	42
July	3	0	2	277	2	2		1,021,861	100	100		70	27	23	26	37	1	36
August	2	1	2	448	9	2		3,385,755	100	100		70	45	97	70	64	1	51
September	6	0	2	385	14	0		6,563,821	100	100		70	48	34	17	70	1	45
October	74	0	3	494	4	0		6,408,886	100	100		70	100	100	100	100	100	137
November	3	0	1	315	4	9		3,440,811	50	100		70	43	67	65	49	0	41
December	7	0	3	262	3	1	298	1,501,962	20	100	90	70	100	100	100	100	100	76
January	7	1	2	369	3	1	342	3,511,820	30	100	87	70	100	100	100	100	100	76
February	20	0	3	323	1	5	424	4,667,006	43	100	95	70	100	100	100	100	100	88
March																		
April																		
May																		
	128	2	20	3,195			424	31,616,917										