ELON UNIVERSITY

Data Breach Response Plan

Written: July 2015

Revised / Approved	**December 13, 2023**
Next Revision / Approval	**December 12, 2024**

Author: Information Security Director

Table of Contents

Plan Overview

Elon University will comply with all international, federal, state and local laws and regulations, as well as applicable industry requirements regarding data breach notification and PII that is Elon Data. Elon University will implement internal controls to monitor, detect, prevent and respond to potential data loss and unauthorized data access as required by applicable laws and regulations.

Elon University has implemented this ***Data Breach Response Plan*** so the University can respond to a potential Data Breach in a coordinated, timely and methodical fashion. This Plan is activated as a result of an incident being classified as a Data Breach (See *Incident Response Plan* and *Incident Response Policy*).

Elon University has also published an ***Incident Response Plan*** that outlines the Purpose; Scope; and Definitions; relevant to suspected or confirmed incidents, including data breaches.

Lastly, Elon University has a ***Written Information Security Program*** that outlines the scope, responsibilities, internal controls, metrics and mechanisms used to secure and protect Elon Facilities, Elon Data, Confidential Information and Elon Assets. The Written Information Security Program contains the following tables of information:

- Roles and Responsibilities (Includes compliance responsibilities)
- List of Information Security policies, plans and procedures
- List of Information Security Control Types, including product and platform
- Information Classification scheme
- List of internal controls

The three documents mentioned above provide foundational, strategic and tactical components and mechanisms that address Data Breaches and potential unauthorized data access issues at Elon University. If a theft, breach or exposure has occurred, the Information Security team and designated Compliance Managers will follow the appropriate process (see Appendix A), depending on the type of data involved. The process will include the following steps:

- Identification
- Escalation
- Secure / Contain
- Remediate
- Recover
- Report
- Lessons Learned

This Plan supersedes any other prior plans, policies or requirements related to these topics and will be reviewed and tested at least annually for potential updates.

Plan Definitions

Breach Notification: Laws require breach notification of individuals or entities affected by a data breach and unauthorized data access. Organizations that have had regulated data breached must notify their customers and other parties about the breach, as well as take specific steps to remedy the situation based on state legislature. Data breach notification laws have two main goals. The first goal is to allow individuals a chance to mitigate risks against data breaches. The second goal is to promote company incentive to strengthen data security.

Compliance Manager(s):

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

Confidential Information: All Elon University proprietary or confidential information, including intellectual property.

Data Breach: the intentional or unintentional release, unauthorized access, use or disclosure of PII data

Data Compliance Team: A team of Compliance Managers called to order in the event of a suspected or confirmed data breach.

Elon Assets: All Elon University-owned or managed networks, network devices, computer systems, applications, or any other technology or computing assets.

Elon Data: 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.

FERPA: Family Educational Rights and Privacy Act

PCI-DSS: Payment Card Industry Data Security Standard

HITECH Act: Health Information Technology for Economic and Clinical Health Act

HIPAA: Health Insurance Portability and Accountability Act

GDPR: EU General Data Protection Regulation

GLBA: Gramm-Leach-Bliley Act

PII: Personally Identifiable Information. Generally, Elon Data, including any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Senior University Leadership (University President and members of Senior Staff): are responsible for ensuring the availability of resources to protect the compliance-related information and Elon Assets and Data and promoting campus-wide compliance to all university policies, as well as regulatory and contractual requirements.

1.0 Identification

Any member of the Elon Community who suspects that a data theft, Data Breach or unauthorized exposure of Elon Data or PII has occurred, must immediately report the incident to their supervisor, the Associate Vice President of Information Technology, or via email to: infosec@elon.edu. A service ticket will be created in Elon's IT ticketing system to track remediation and response activities by the Elon response teams.

Once reported, the Elon response team will investigate the incident and determine if a reportable Data Breach has occurred.

Upon the identification and classification of an actual Data Breach, the Incident Response Leader (See Incident Response Plan) will contact the CIO. The CIO will convene the Data Compliance Team, ensuring the appropriate Compliance Manager(s) are briefed on the cyber incident and able to assist with recovery. In addition to the CIO and Compliance Manager(s), it is recommended that each response team include representatives from the following areas:

- Information Technology
- University Communications
- Risk Management
- The affected unit or department that uses the involved system or output or whose data may have been breached or exposed
- Additional individuals as deemed necessary by the Compliance Manager
- Outside counsel (if required)

Documentation is a crucial part of the Data Breach Response process. The determination of the severity of the incident may not be obvious during the initial phase of the response. Failure to document all activity beginning at the first phase of the response may result in loss of information and/or actions. It should always be assumed that an incident may result in legal review as required in a regulatory review, civil action, or criminal investigation. As such, all activities should be recorded in the original ticket created by the Compliance Manager or Information Security. Below is the type of information that should be recorded in the ticket:

- The time and date that the event occurred.
- The level of severity of the impact and/or potential impact.
- A summary of the event.
- The system and type of data involved.
- Explain which policy / regulation was violated and what caused the incident.
- List all corrective actions and remediation steps and activities in the assigned ticket.

Note that certain communications, reports and investigation records should be protected by attorney-client privilege when legal counsel is involved in the response process. Accordingly, all such communications, documentation and working drafts should be marked as “Attorney-Client Privileged and Confidential” unless or until instructed otherwise by Elon Senior Leadership of legal counsel.

2.0 Escalation

Once the cyber incident has been identified, an evaluation of the issue will be conducted by the responsible Compliance Manager with assistance from Elon's Risk Management Office, CIO and the Data Breach Response Team. Appendix B is a process diagram the shows the relationship and escalation path for incidents that impact the Problem Response Plan, the Data Compliance Team and the Emergency Operations Center (EOC). The Data Compliance Team will determine if Elon's Emergency Operation's Center should be readied.

NOTE: In the event that criminal activity is suspected, immediately contact Elon University Campus Safety & Police and notify them of the situation.

During this phase, the following activities should occur:

- Determination by the Data Breach Team if law enforcement is needed.
- Elon's Risk Management Office and/or the Director of Information Security will determine if the Data Breach requires notification to Elon's Insurance carrier (Allied World). If so, either the Risk Management Office or the Director of Information Security will contact:

  Allied World Breach Consultant
  Incident Evaluation Hotline # 844-736-2428 or
  AWCyberEvent@awac.com for a breach consultation with no retention applicable
  NOTE: Allied World Breach Consultant can provide information and advice to Elon regarding security policy coverage, and recommended remediation steps, outside vendor assistance and notifications to regulatory bodies if needed. The AWB consultant can also be contacted throughout the handling of the breach for advice and remediation strategy. The cost of this service is included in the insurance premium paid for the policy.

- The Data Compliance Team will notify University Senior Leaders as appropriate, and the following departments if appropriate:

Data Type	Areas to Notify
Financial information, including but not limited to credit card numbers, bank account numbers, investment information, grant information, and budget information	Accounting
Information about individual employees, including but not limited to social security numbers	Human Resources
Student financial information	Admissions, Bursar, Registrar
Student information protected by FERPA	Registrar, Provost
Student health information	Student Life
Student information not listed above	Student Life, University Communications, Provost
Research data	Provost
Information Containing PHI under HIPAA Privacy Rule	Office of the Dean of Students
PII concerning faculty	Human Resources, Provost, Risk Management
PII concerning donors or unreleased information about gifts received	Advancement

Data Type	Areas to Notify
Payroll information	Controller and Human Resources

- Information Technology will review impacted technical controls and system configurations
- Affected department personnel will brief staff on current issues

Note: Any action taken on an affected system by the system administrator to investigate an event could greatly affect and even alter evidence of malware and unauthorized access and may affect the use or security of the system or network. At the first indication of the need for computer forensics analysis, Information Security will contact a forensics specialist to investigate and advise on next steps and ensure the appropriate Elon Data Breach Team members are notified.

- Information Security will be responsible for coordinating the use of computer forensics for one or more phases of this plan. Computer forensics can be utilized to collect and recover destroyed data, create forensic images of affected systems, analyze logs and data for suspicious activity, and coordinate with law enforcement if necessary.

3.0 Secure and Contain

The purpose of this step is to minimize the potential impact of the incident on Elon Data, Confidential Information and Elon Assets, with an emphasis on acting swiftly to prevent a worsening situation. At this point, the Data Breach Response Team should be working through an Action Plan to secure the data and contain the exposure. The Data Breach Response Team Leader should consider the following steps, while also preserving evidence, log files and other artifacts crucial to retrospective forensic investigation, to identify affected persons or data, etc.:

- Secure the area where the incident occurred.
- Disable access to data that has been impacted.
- Estimate the impact of damage.
- Estimate the impact of restoration.
- Change authentication credentials.
- Preserve evidence.
- Do not alter affected data.
- Back up information systems.
- Document events (include date, time, and explanation of event/events).
- Disconnect the affected and related systems or networks from Internet access.
- Document date and time the breach occurred, what files the user was accessing at the time of the breach, the breach team member contacted, and actions taken to secure data.
- If appropriate, detect and remove the malware or other information related to the breach.
- Review virus/malware/other protective software to review system vulnerabilities and increase the level of protection for the system.
- If appropriate, reimage the system and restore from backup files.

4.0 Remediate

The purpose of this step is to mitigate the potential impact of the incident. The Data Breach Response Team should consider the following steps:

- Determine the root cause of the Data Breach
    a. If the incident was caused by a virus, Trojan, or malware, make sure all virus definitions are up to date and verify that the antivirus application is functioning properly on all systems.
    b. If the incident occurred because of an unpatched system or software, verify that all similar systems and all relevant software are reviewed. Also, make sure all software updates are applied.
    c. If the incident was a result of human error, educate the persons involved.
    d. If the incident was a result of a third-party service provider, Elon will re-evaluate the vendor contract for expected compensation and assistance.
    e. If the incident was the result of an application vulnerability, Elon will take the necessary steps to close the vulnerability as quickly as possible.
- Use any information gathered during this phase to secure other similar systems in the network that have yet to be affected by the incident.
- Put proper measures in place to protect all network systems and applications from similar events.
- Defend and protect systems, applications, networks, and data against unauthorized activity and adverse authorized activity.
- If necessary, restore and/or repair damaged information systems affected during the incident.

5.0 Recovery

The purpose of this step is to restore systems to original functioning status and restore customer service. Included in this step is the testing and verification that all systems are operating normally and are fully functional (as in pre-incident). The Compliance Manager and Data Breach Team Leader should ensure the Service Ticket has been updated with all the Recovery and Remediation steps taken.

In addition, steps may need to be taken to comply with various regulations. These steps could include the following but will be determined by legal requirements (confer with outside counsel as applicable to ensure alignment with all state and federal requirements):

- Preparing external communications and notifying appropriate authorities
- Notifying affected individuals via email and postal mail
- Creating a Data Breach web site with breach information for internal and external communications
- Activating a toll-free number to answer questions for external communications
- Activating a special email address for internal and external communications

6.0 Report

The purpose of this step is to ensure all reporting, notifications and communication requirements have been met. The Compliance Manager and Data Breach Team Leader should ensure the appropriate reports, ticket updates and notifications are created and disseminated. The types of reporting, notifications and communication requirements may include:

- Inform University Senior Leadership that the Data Breach has been resolved.
- Inform all other relevant parties involved that the Data Breach has been resolved.
- Ensure the Data Breach is fully documented in the Service Ticket (this can be used to generate detailed Data Breach reports if required).
- Ensure the legal requirements for Breach Notification have been met.

- Communicate to appropriate constituency and departmental leaders.
- Complete a “Lesson Learned” report in preparation for closure of the incident.

7.0 Lessons Learned

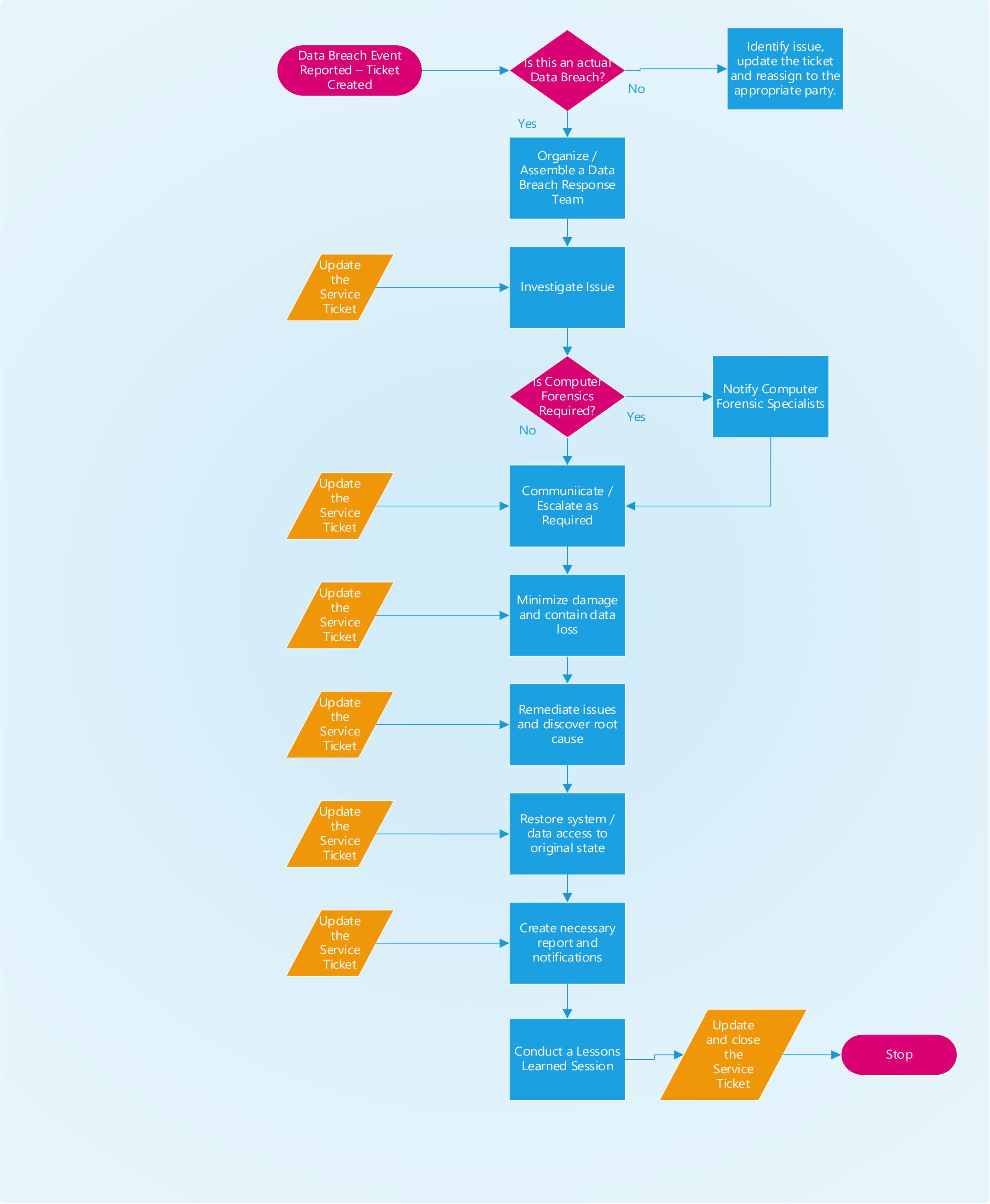
The objective of this section is to conduct a closing meeting to discuss the Data Breach to determine potential enhancements in policies and/or procedures to reduce likelihood of this type of incident in the future. The CIO and Compliance Manager will be responsible for coordinating which individuals are to attend the meeting.

Questions and comments to be included in the meeting:

- Was there documentation of every event?
- Discuss what, when, where, how, and why of the incident.
- What happened? Worm? Virus? Theft? Hacker? Other?
- Why did it happen? Are there vulnerable areas that need to be addressed?
- Where did this incident occur? Was it being monitored?
- How did the incident occur? What was the severity? Was it minimal, serious, or critical?
- Are there potential weaknesses in the system that need to be remediated?
- Why did this happen? Was it an internal lapse? If so, how can it be fixed? Was it an unforeseeable external occurrence? If so, how can it be avoided in the future?
- Discuss what preventative measures could be taken to avoid the incident in the future. Perhaps additional procedures or a change in policy, if needed.
- Inform employees of safe network security practices as to avoid potential vulnerabilities.

After consolidating the information obtained from the meeting, further steps may be required to document, implement, and enforce the corrective courses of action.

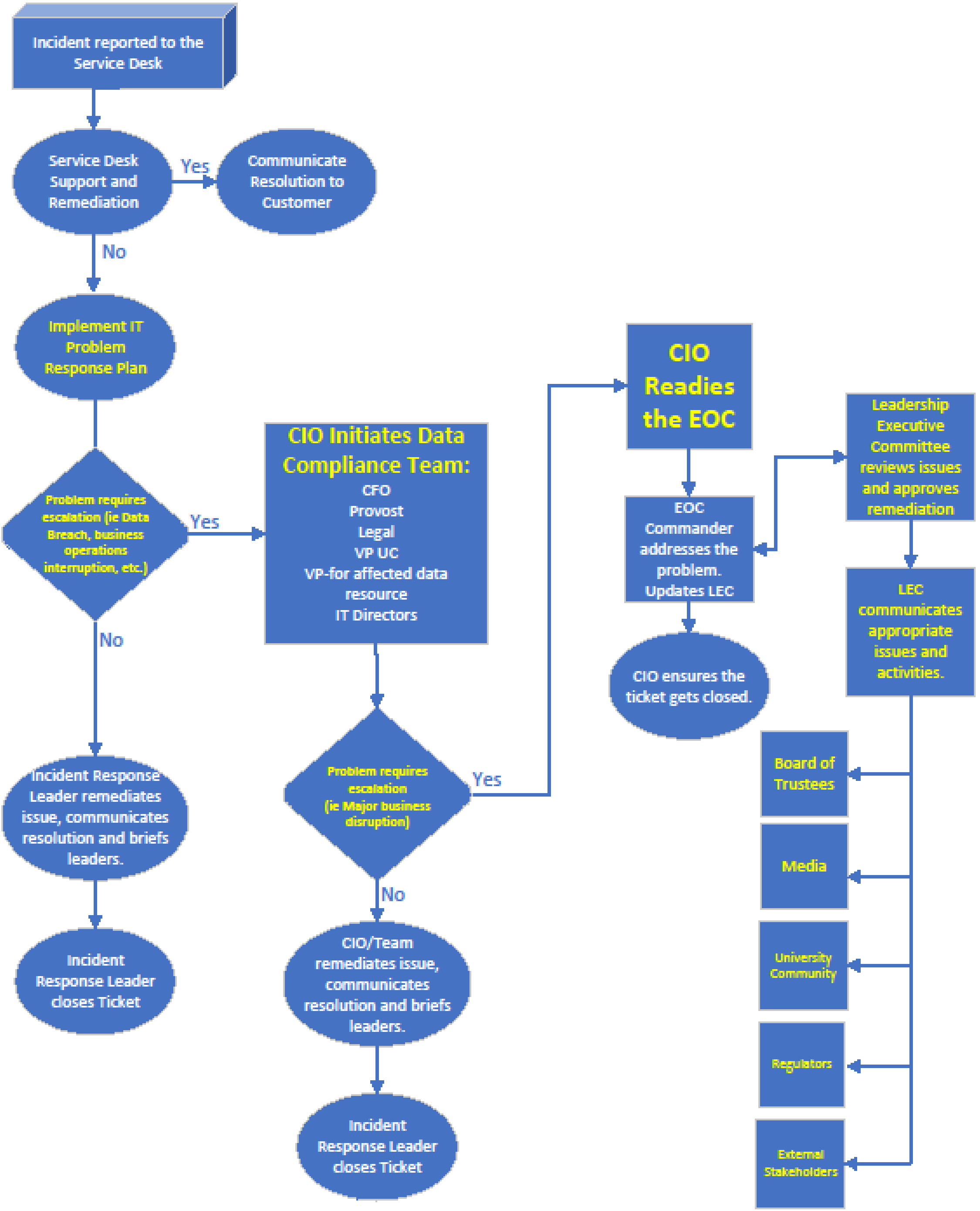
Appendix A - Process Flow Chart


Data Breach Event Reported – Ticket Created
Is this an actual Data Breach?
No
Identify issue, update the ticket and reassign to the appropriate party.
Yes
Organize / Assemble a Data Breach Response Team
Update the Service Ticket
Investigate Issue
Is Computer Forensics Required?
Yes
Notify Computer Forensic Specialists
No
Update the Service Ticket
Communiicate / Escalate as Required
Update the Service Ticket
Minimize damage and contain data loss
Update the Service Ticket
Remediate issues and discover root cause
Update the Service Ticket
Restore system / data access to original state
Update the Service Ticket
Create necessary report and notifications
Conduct a Lessons Learned Session
Update and close the Service Ticket
Stop

Appendix B – Escalation Process

Revised 08/2022

Problem/Incident Resolution Escalation Process


Incident reported to the Service Desk
Service Desk Support and Remediation
Yes
Communicate Resolution to Customer
No
Implement IT Problem Response Plan
Problem requires escalation (ie Data Breach, business operations interruption, etc.)
Yes
CIO Initiates Data Compliance Team:
CFO
Provost
Legal
VP UC
VP-for affected data resource
IT Directors
No
Incident Response Leader remediates issue, communicates resolution and briefs leaders.
Incident Response Leader closes Ticket
Problem requires escalation (ie Major business disruption)
Yes
No
CIO/Team remediates issue, communicates resolution and briefs leaders.
Incident Response Leader closes Ticket
CIO Readies the EOC
EOC Commander addresses the problem. Updates LEC
CIO ensures the ticket gets closed.
Leadership Executive Committee reviews issues and approves remediation
LEC communicates appropriate issues and activities.
Board of Trustees
Media
University Community
Regulators
External Stakeholders

Appendix C – Data Breach Response Contacts

Outside consultants may also be activated and included in the CSIRT by the Incident Response Leader. Outside consultants include but are not limited to:

1. **Rusty Gilmore & Associates (Forensic Investigator Risk Management Associates)**

Contact	Russell Gilmore
During business hours (Monday-Friday, 8:00 AM-5:00 PM)	919-834-8584 ext. 315
After business hours (Please leave message)	919-417-1787
Email	rgilmore@rmasecurity.com

2. **TCDI (Forensic Investigation and Penetration Testing)**

Contact	Eric Vanderburg
During business hours (Monday-Friday, 8:00 AM-5:00 PM)	440-376-2398
After business hours (Please leave message)	440-376-2398
Email	e_vanderburg@tcdi.com

3. **Allied World Insurance (Elon's cyber insurance provider)**

Contact	Incident Evaluation Hotline
During business hours (Monday-Friday, 8:00 AM-5:00 PM)	1-844-736-2428
After business hours (Please leave message)	1-844-736-2428
Email	AWCyberEvent@awac.com
To initiate Service you must provide: • the full name of the insured organization • the name and phone number of the individual authorized to discuss this matter, and if available • the insurance policy number.	

4. **IT Escalation**

First Contact	Christopher Waters	336-633-8683
Second Contact	Patrick Donohue	336-269-9015
Third Contact	Gary Sheehan	336-317-6996