Problem Response Plan

Written: July 2015

Revised / Approved	12/13/2023
Next Review / Approval	12/13/2024

Author: Information Security Director

Table of Contents

Revision Table

Effective Date	Author	Version	Approved	Change Reference
07/15/2015	Director – Information Security	1.0	Christopher Waters	Initial Program Guide
12/13/2021	Gary Sheehan	2.0	Christopher Waters	Formatting / Legal Review
12/12/2022	Gary Sheehan	2.1	Christopher Waters	Formatting / Added Escalation Diagram

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

This Problem Response Plan is the documentation of a predetermined set of instructions and procedures to detect, respond to, and limit the potential impact of malicious cyber-attacks or similar incidents against Elon University's information system/systems, including Elon Facilities, Elon Assets and Elon Data. This plan was written in accordance with the accepted practices and regulations of the National Institute of Standards and Technology. This Incident Response Plan is designed to provide a guide to address suspected or real incidents that may potentially compromise the integrity of the University's network, systems, or data. The goal of this Plan is to provide guidance so that all aspects of a perceived or actual threat are managed thoroughly.

This Plan serves as a guideline for Elon University and the Elon Community to protect Elon Assets, Confidential Information and Elon Data from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:

1) Integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity;
2) Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
3) Availability, which means ensuring timely and reliable access to and use of information.

Elon's Incident Response Plan follows a standard approach to incident response and includes the following activities:

- Identification / Escalation (escalation is this plan refers to contacting the next level of support due to the seriousness or impact of the event)
- Containment
- Remediation
- Recovery
- Review

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.

Identification / Escalation

Upon identification of a suspicious event (the creation and submission of a service ticket) an evaluation of the issue will be conducted by the Service Desk with approval of the Director. After the initial evaluation, the Service Desk Representative will perform one of the following:

1. Address and remediate the issue / event / incident and close the ticket.
2. Escalate the issue for further evaluation and identification to Enterprise Applications, TLT, System Administration, Network Support or Information Security. If the ticket is escalated to another group for remediation, the Service Desk will update the ticket to ensure it can be tracked as an "incident" rather than a support call.

3. Create a Problem Ticket and execute the Problem Response Process by escalating the problem to the appropriate Director. ***The Director will assume responsibility for containment, remediation, and recovery on the problem.***

NOTE: All incidents that include a suspected Data Breach issue or are identified as a Data Breach MUST be escalated to the appropriate group Director for containment, remediation and recovery in accordance with the Elon Data Breach Response Plan.

Once the incident has been identified and escalated, work can begin on the subsequent response activities. The Director is responsible for:

1. Identifying the appropriate Incident Response Team (IRT) with the appropriate technical and communication skills to contain, remediate and recover from the incident. Typically, an IRT will have the following member roles:
    a. Incident Response Leader (Generally, the Director assigned the problem)
    b. Technical Communication Liaison (Generally the Assistant Director)
    c. One or more technology specialists
2. Ensuring proper communication occurs to all relevant parties about the event or incident, and when necessary, ensuring the event information is escalated to the necessary University Senior Leadership and relevant stakeholders.
3. Ensuring the incident ticket is updated with all relevant information about the incident or event so proper follow-up can be executed if needed. Documentation is a crucial part of the incident Response. 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 a potential incident may result in legal review as required in a regulatory review, civil action, or criminal investigation. 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.

The Director will be responsible for coordinating the use of computer forensics personal and/or technology 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. When contract computer forensics services are necessary, the contractor will be assigned as part of the response team and will report to the Director.

The Service Desk Representative and the Director should ensure all documentation regarding the identification, escalation, containment, remediation and recovery from the event or incident is recorded in the ticket. Information that should be recorded in the ticket includes, but should not be limited to:

- Time and date that the event occurred.
- Level of severity of the impact and/or potential impact.
- Summary of the event.
- Name the system being targeted (include operating system, IP address and location).
- Attempted corrective actions and whether or not they were successful.

In the event the ticket system is not available during the course of this incident, a template has been devised (Appendix A) that can be used to record the necessary information until the ticket system is available. Once the ticket system is available the document can be uploaded as an attachment to the problem ticket.

Appendix A is a process flow diagram that shows the escalation process and relationship between the Problem Response Process, the Data Compliance Team and the Emergency Operations Center.

Containment

The purpose of this step is to minimize the potential impact of an incident, with an emphasis on acting swiftly to prevent a worsening situation. Once assigned the problem, the Director should convene an Incident Response Team (IRT) to assist with containment, remediation and recovery. The IRT will likely be needed to work through the containment, remediation and recovery phases for the incident.

To help minimize the risk and ensure containment of the incident, the following activities should be considered during this phase while also preserving evidence, log files and other artifacts crucial to retrospective forensic investigation, to identify affected persons or data:

- 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
- Communicate to relevant stakeholders

If the severity of the incident/event is critical, the Director must notify Elon University administration as soon as possible. In the event that criminal activity is suspected, the Director must immediately contact Elon University Campus Safety & Police and notify them of the situation.

Remediate and Eradicate

During this phase the IRT should determine the root cause of the incident and formulate and execute a plan to remediate the incident. Examples of remediation actives are:

- 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.
- 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.
- If the incident is related to a vulnerability, then an analysis of the affected system as it relates to the vulnerability of the systems, applications, network, and data should be conducted.
- If the incident was a Data Breach, then the Data Breach Response Plan should be implemented as soon as possible.
- If the incident was related to the loss of utilities or a third-party service the provider should be contacted immediately.

Remediation and eradication can take many forms based on the nature and severity of the incident. Problem Response Playbooks will be developed to help quickly address remediation efforts of known vulnerabilities, incidents and events.

Communication and documentation are critical components within this phase of the plan.

Recovery

During this phase the IRT should implement steps to ensure the data, application(s), systems, business process, or business procedures are restored to their original functioning status. To ensure a complete recovery the IRT should:

- Compare the affected resource against original baseline
- Ensure business units test the service/system to verify functionality
- Restore the affected resource(s) to production environment status
- Perform ongoing system monitoring to ensure system integrity and detect incident recurrence
- Ensure all stakeholders involved in the incident are informed about the recovery process
- Communicate to appropriate constituency and departmental leaders
- Continue to monitor the affected systems / applications and relevant network activities

Lessons Learned

The objective of this phase is to discuss the incident to determine potential enhancements in policies and/or procedures to reduce likelihood of this type of incident in the future.

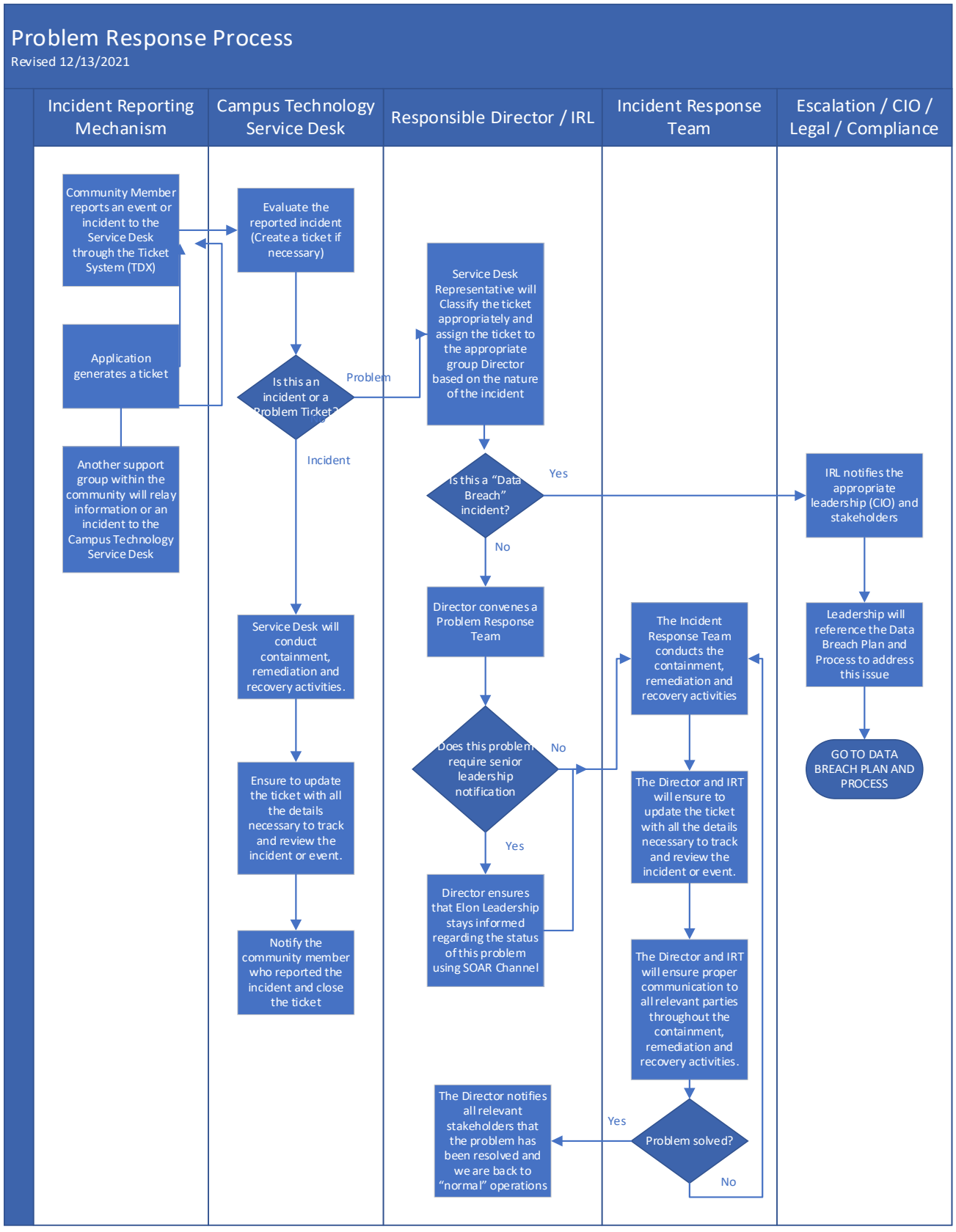
At an appropriate time, the Director responsible for the incident should schedule a “Lessons Learned” meeting with the IRT and affected stakeholders to discuss the problem that occurred and determine if preventative measures could be taken to avoid the incident in the future.

On a quarterly basis, the Information Security Advisory Committee (ISAC) will be responsible for reviewing the incidents over the past 90 days and determining if changes to technology, process policy or procedures are required to prevent further incidents. The Director of Information Security will be responsible for facilitating this discussion. Questions and comments the ISAC can ponder can include:

- 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?
- 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 the results from the “Lessons Learned” follow-up meeting. Perhaps additional procedures or a change in policy, if needed.

After consolidating the information obtained from the meeting, the ISAC may make recommendations to the Information Security Executive Committee for updates or upgrades to current technologies, processes, policies or procedures.

Problem Response Procedural Flow Chart



Emergency Resources

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

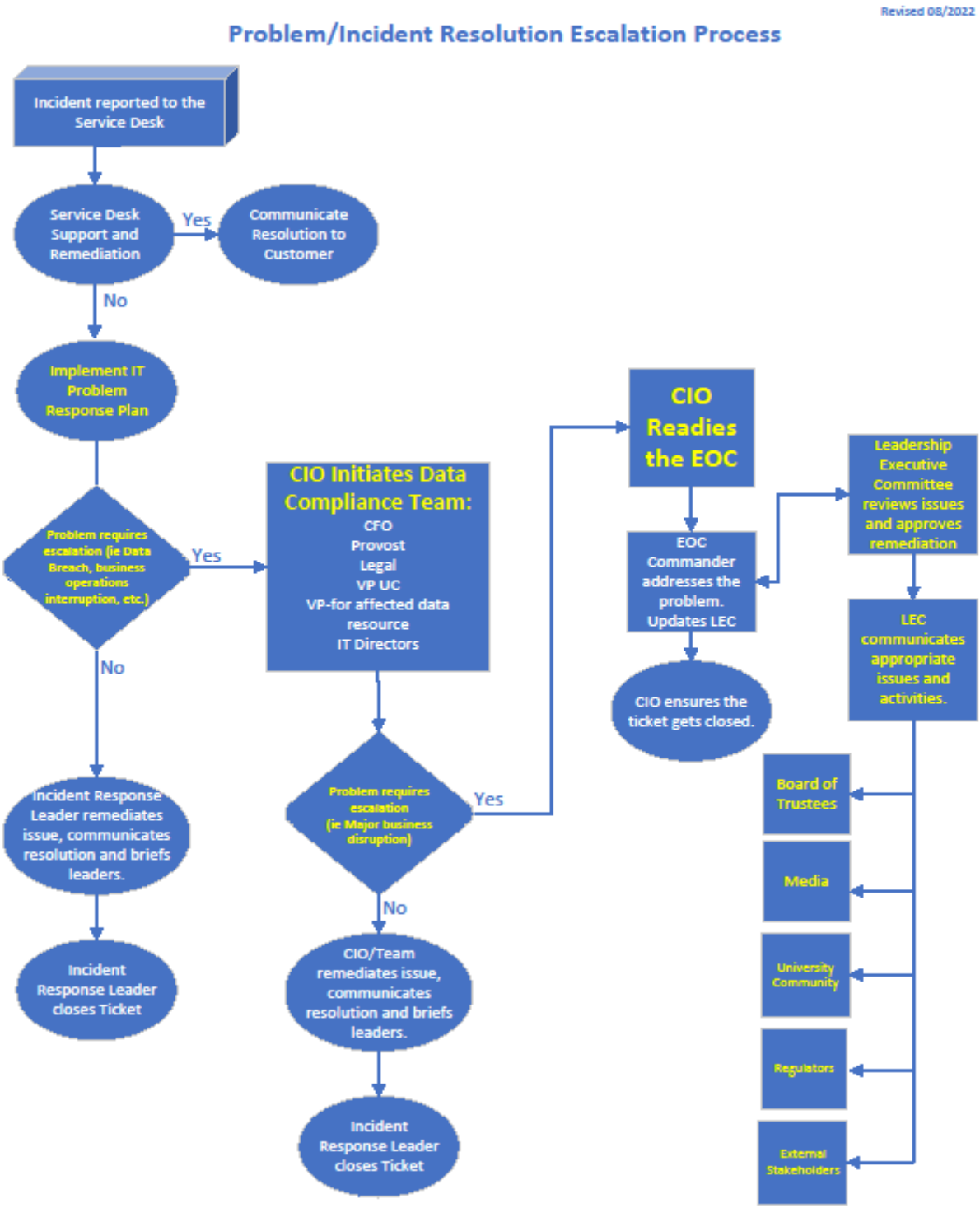
3. **Allied World Insurance (Elon's cyber insurance provider)**

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

APPENDIX A


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
No
CIO Initiates Data Compliance Team:
CFO
Provost
Legal
VP UC
VP-for affected data resource
IT Directors
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