TECHNICAL COLLEGE
OF THE LOWCOUNTRY

PROCEDURE: Incident Response Plan
Number: 2.3.2.4

Responsibility:	Administrative Services (Information Technology Department)
Last Updated:	November 1, 2023
Related Policy:	2.3.2 Information Technology Security

_____

President

Purpose:

This procedure outlines the framework the Technical College of the Lowcountry will use to respond when an Information Security Incident is deemed to have occurred.

Procedure:

Preparation

1. Establish an incident response team consisting of representatives from IT, security, legal, and management departments.
2. Develop a formal incident response plan that outlines roles and responsibilities, communication procedures, escalation paths, and incident categories.
3. Conduct regular training and simulations for the incident response team to ensure that they are prepared to handle cyber attacks.
4. Identify critical assets and data and create backups to ensure their availability in case of a cyber attack.
5. Implement network segmentation to limit the spread of a cyber attack.
6. Establish relationships with external partners such as law enforcement and third-party incident responders.
7. Regularly review and update this incident response plan to ensure that it remains effective.

Detection

1. Use intrusion detection and prevention systems, security information and event management (SIEM), and other monitoring tools to detect potential security incidents.
2. Establish baseline behavior for normal network activity and use monitoring tools to

identify deviations from the norm.
3. Conduct regular vulnerability assessments and penetration testing to identify weaknesses in the network.
4. Train employees on cyber security best practices and awareness to detect and report potential threats.
5. Review logs and alerts generated by security systems to identify potential threats.

Analysis

1. Verify the security incident to determine whether it is a false positive or a genuine security incident.
2. Determine the scope and impact of the security incident.
3. Collect and analyze data and evidence to identify the cause and root of the security incident.
4. Communicate with external partners such as law enforcement or third-party incident responders as needed.

Containment

1. Isolate the affected systems and devices from the network to prevent the spread of the attack.
2. Implement security measures to stop or contain the attack, such as blocking IP addresses, disabling accounts, or shutting down systems.
3. Collect evidence for forensic analysis to determine the cause and scope of the attack.

Eradication

1. Remove any malware or malicious code from the affected systems and devices.
2. Patch any vulnerabilities that were exploited by the attacker.
3. Verify that the affected systems are clean and secure before returning them to the network.

Recovery

1. Restore any data or systems that were affected by the attack using the backups created during preparation.
2. Conduct a post-incident review to identify areas for improvement and update the incident response plan accordingly.
3. Reassess the network security posture to ensure that it remains strong and effective against future attacks.
4. Communicate the incident and its resolution to all stakeholders and customers as appropriate.

Post-Incident Activities

1. Conduct a lessons learned session to identify areas for improvement and update the incident response plan accordingly.
2. Update policies and procedures to address any deficiencies that were identified during the incident response.
3. Conduct a review of the organization's security controls to ensure that they remain effective against current and emerging threats.
4. Train employees on any changes made to policies, procedures, or security controls.