Checklist of significant steps for Incident Response and Handling

a. **Preparation — Includes documentation, testing, training and other preparatory activities.**

- ❑ Review and adopt the University Incident response plan, or use it to create your own.
- ❑ Create a prioritized list of critical information assets to the functioning of your Unit.
- ❑ Ensure a communication plan is in place for each severity of the incident.
- ❑ Identify who will be on the CSIRT team; this can be specific people or identified positions.
- ❑ Identify any tools needed for communication, artifact collection, or other activities.
- ❑ Document as much as possible ahead of time and ensure that the files are somewhere it will be available when needed.
- ❑ Train staff or faculty on how to identify an incident and how to report it. The CSIRT team members run a tabletop exercise to understand their role and responsibilities in the process.
- ❑ If available, identify and review the Unit's IT and Business Continuity Plans
- ❑ Review the plan and documentation annually to ensure it stays up to date.

b. **Identification —This identifies what data, devices, or systems were damaged, accessed, or exposed as part of the breach. Additionally includes the collection of logs, system images, and other artifacts. Activation of the CSIRT happens at this time.**

- ❑ Understand what has happened, what assets are affected, and the overall impact
- ❑ Begin documenting the incident timeline, any actions taken, and artifacts collected. This may be the best estimate for the timeline, as details may not be available at this point.
- ❑ Classify the data and criticality of impacted assets
- ❑ Determine the severity of the incident
- ❑ Assemble a Security Incident Response Team (CSIRT) and assign an Incident Manager
- ❑ Activate the communication channels needed for the CSIRT team and others that must be notified.
- ❑ Determine if a breach coach or external forensics is needed
- ❑ Collect Logs related to the event. These include but are not limited to those from:
- ❑ Network devices
- ❑ Centralized logging (SIEM, Syslog Servers)
- ❑ Authentication sources (LDAP, Active Directory, RADIUS, etc.)

c. **Containment — Initial short-term containment of the incident, primarily this will be disconnecting devices or networks to limit any spread of malware or malicious activity. Start Short-term containment to stop the attack/issue. This includes:**

- ❑ Isolate affected assets – disconnect from the network but do not power off!
- ❑ If available, take the appropriate measures to restore services according to the Unit's IT and Business Continuity Plans.
- ❑ Assess risk to other systems
- ❑ Apply additional interim mitigations, additions to monitoring, etc.
- ❑ Collect evidence for additional review, and any possible legal proceedings
- ❑ Create forensics images of the hard drives and memory
- ❑ Take a snapshot of Virtual machines to preserve the current state.
- ❑ Retrieve hard copies of any disclosed personal information.
- ❑ Continue to document findings
- ❑ Report results to CSIRT

d. **Eradication— Identify the root cause of the incident. Remove malware, malicious code and vulnerabilities from all affected systems using the identification step's collected information.**

- ❑ Identify the root cause — It's critical to understand what caused the incident to prevent future compromises for the same reason.
- ❑ Scan for malware — use anti-malware software or Next-Generation Antivirus (NGAV) if available to help determine the root cause.
- ❑ Restore, Rebuild, or Replace — A compromised system shall never be cleaned and restored to production unless there is no other option.
- ❑ Restoring a system from backup can be an effective method to get a system back into production quickly; however, any backups used must be from before the compromise occurred.
- ❑ Rebuilding a system from scratch is more time-consuming but ensures a clean system.
- ❑ Replacing an old system with newer versions of the OS and applications is more time-consuming but effective to ensure a system is up to date and secure.

e. **Recovery — Return systems carefully back to production status, ensuring mitigation of the root cause occurs first.**

- ❑ Fully patch all systems before connecting to the network.
- ❑ Change all local system and user passwords on affected systems before redeployment. This activity shall extend to any centralized accounts that used the system as well.
- ❑ All passwords and private keys stored on the system used to access other systems must be changed.
- ❑ Harden a system to a well-documented standard. (i.e. CIS Benchmarks)
- ❑ Scan for and remediate discovered vulnerabilities before redeployment.
- ❑ Document any exceptions for vulnerabilities that cannot be remediated, including the compensating controls used instead.
- ❑ Improve monitoring to help stop any recurrence of the incident.

f. Lessons learned — Review the root cause of the incident and identify opportunities to improve detection and defences to lessen a reoccurrence chance. Also, review the process of dealing with the incident and determine any improvements there as well.

- ❑ Hold a lessons learned session with stakeholders and CSIRT members to identify opportunities to improve detection of malicious activity, defences, and the incident response process.
- ❑ Create a report based on that session's results with the issues identified and recommendations for improvement. Ensure management views the report if they were not involved with the lessons learned session.
- ❑ Create a plan to implement any recommended changes and improvements with target dates for completion.