Hospital X

Incident Response Plan

Version 1.0

INCIDENT RESPONSE CHECKLIST

Documentation note: Pay special attention to the **bold** statements throughout the checklist when documenting incident notes. In the incident presentation to your CISO, only document the steps required within the template as requested.

Step 0	Indicator of Compromise validated and incident confirmed	☐
Step 1	**Document the entity who discovers the incident.** Possible sources are below. The contact procedure and contact list should be updated quarterly: • Helpdesk • Intrusion detection monitoring personnel • A system administrator • A firewall administrator • A business partner • A manager • End users • The security department or a security person. • An outside source.	☐
Step 2	The incident response team gathers, investigates the incident using a checklist, and determines if the incident should be escalated based on impact. **Consider and answer the following questions:** Impact Considerations a) What is the indicator of compromise? b) What is the potential impact of the incident? c) Name of system being targeted, the operating system, and the IP address. (use lab environment machine)	☐
Step 3	**Consider and answer the following questions on triage:** a) Is the incident confirmed? Or an indicator of compromise that's not yet verified? b) Is the incident contained already or still in progress? c) Is the response urgent? d) Will any response alert the attacker and if so, do we care? e) What type of incident is this? Example: virus, worm, intrusion	☐
Step 4	**Is safety or human life at immediate risk?** - the IR team should ensure their own survival and survival of the staff as a priority.	☐

Step 5	As soon as possible, the regional threat manager at 999-999-9999 and the security operations center at 999-999-9999 of the incident. They will coordinate communication with other internal and external stakeholders.	☐
Step 6	An incident ticket should be created by the IR team. The incident should be categorized into the highest applicable level of one of the following groups. **Which category ticket should be opened and why?** a) Category one - A threat to public safety or life. b) Category two - A threat to sensitive data c) Category three - A threat to computer systems d) Category four - A disruption of services	☐
Step 7	**Which applicable procedure should the IR team follow based on their understanding of the incident?** a) Malware response procedure b) Virus response procedure c) System failure procedure d) Insider threat procedure e) Physical property theft response procedure f) Website denial of service response procedure g) Database or file denial of service response procedure h) Spyware response procedure The team may create additional procedures which are not foreseen in this document. If there is no applicable procedure in place, the team must document what was done and later establish a procedure for the incident. In the recent more commonly occurring event of ransomware (a form of malware) to recover from the incident isolate the systems infected by the ransomware, wipe them clean, and restore systems fully from backups.	☐
Step 8	IR team members may use digital forensic techniques, including reviewing system logs, checking computer activity, and interviewing witnesses to determine how the incident was caused. Only authorized personnel should be performing interviews or examining evidence, and the authorized personnel may vary by situation and the organization. **Document whether or not you're able to check the logs. If unable, document alternatives to understand what caused the incident.**	☐
Step 9	**Which recommended changes should the IR team make to prevent the occurrence from happening again or infecting other systems**. Upon approval changes are to be implemented. Action examples are included below however, you should develop recommendations tailored to the attack at hand. a) Re-install the affected system(s) from scratch and restore data from backups if necessary. Preserve evidence before doing this. b) Make users change passwords if passwords may have been sniffed. c) Ensure the system has been hardened by turning off or uninstalling unused services. d) Ensure the system is fully patched. e) Be sure real time virus protection and intrusion detection is running. f) Be sure the system is logging the correct events and to the proper level.	☐
Step 10	Documentation—the **f**ollowing shall be documented**:** a) How the incident was discovered. b) The category of the incident. c) How the incident occurred, whether through email, firewall, etc. d) Where the attack came from, such as IP addresses and other related information about the attacker.	☐

	e) What the response plan was. f) What was done in response? g) Whether the response was effective.	
Step 11	Evidence Preservation—make copies of logs, email, and other communication. Keep lists of witnesses. Keep evidence as long as necessary to complete prosecution and beyond in case of an appeal.	☐
Step 12	**Review response and update policies—plan and take preventative steps so the intrusion can't happen again. Which updates do you recommend and why?** a) Consider whether an additional policy or technology could have prevented the intrusion. b) Was the incident response appropriate? How could it be improved? c) Were the incident-response procedures detailed and did they cover the entire situation? How can they be improved? d) What changes can be made to prevent a re-infection? e) What lessons have been learned from this experience?	☐
Step 13	The IR team continually follows the IR plan and business continuity plans continue until the incident has been resolved.	☐