CYBER INCIDENT SYSTEM RESTORATION CHECKLIST

Immediate actions of the IT recovery team will include identifying and isolating the threat, and assessing damage/impact to hospital operation, for rapid restoration of services.

☐ Consider running hardware, backing up, or mirroring data at an alternate (non-affected, secure) site.

☐ Identify which vendors can provide additional support and assist with recovery efforts, including provision of “hot sites,” additional resources, equipment, skilled staff; assistance with system recalibration/reconfiguration; data testing/validation.

☐ Use previous BIA or application mapping data to organize restoration needs and prioritize services. Have a process in place to adjust recovery priority levels as information emerges.

☐ Communicate any changes to the restoration process and priority levels early and often to data custodians, relevant department representatives, incident command leads. Ensure data custodians remain part of the recovery process as systems are brought back online.

☐ Establish a daily stand-up meeting to discuss recovery status and barriers to completion. Ensure representatives from clinical and non-clinical departments are engaged to provide and relay status changes back to staff. Ensure staff know the period of time a system will be non-operational.

☐ Provide brief daily system restoration status updates to all departments that includes information about available systems those which are not fully functional.

☐ Create a “restoration matrix” (or spreadsheet) to log the status (e.g., fully versus partially operational, restricted) of all systems being restored. In the document, outline capabilities that are working and features that are not working or are restricted. Appoint someone to update data and store in a centrally accessible location (e.g., collaboration tool, knowledge center). Use the status reports and restoration matrix to assess recovery progress and adjust recovery efforts accordingly.

☐ Use the official system name AND the laymen/common operational name for staff that are unfamiliar with IT jargon in all reports and status briefs.

☐ Set up an email for stakeholders to submit new priorities/issues as they are identified. Email should go directly to technical recovery leads (IT department) so they can be included in daily standup meetings and assessed for placement in the backlog. Ensure new restoration requests are channeled solely through the recovery lead to prevent IT personnel from being disrupted by new issues, concerns. Shielding teams from daily operational discussions will speed recovery time.

☐ Appoint a person who is highly familiar with the system/application to test and validate it once it is brought back online. Testers should verify the system is operating as expected and identify/document issues. Ensure all bugs are logged and reported back to IT and Incident Command. Include the validation outcome on the status matrix.

☐ When biomedical equipment has been restored, consider waiting to re-integrate into operations until it is confirmed devices have been properly recalibrated and outputs are validated. When possible set a standard waiting period. Consider engaging the vendor to assist with restoration.

☐ Release recovered departments to smaller units first for initial testing before fully releasing. Have a process to verify results are accurate and consistent and that data output is being disseminated to the proper systems/applications.