

Business Continuity Information Security Questions

The university is increasingly reliant upon information technology and computers to perform everyday business with no fallback to a manual/paper practice. The following questions will aid in emergency planning by helping you to identify those information assets that you need to continue your work when these assets become negatively affected by a crisis. Your IT support staff may be best able to work with you to create the documented plans and processes needed to ensure continuity of your business practices, so be sure to include them or consult them when addressing these items.

Any documents created by you or your area to address these questions must be noted in the organization business continuity document and become a part of the formal business continuity action plan.

The university IT security group (security@osu.edu), our partners in the business continuity development process, can address any questions or give necessary clarification on the content or intent of these questions. Please include the business continuity team in these communications as we manage the overall continuity planning process.

Confidentiality:

Action	Completed?	Documentation Location
1. Document the individuals and roles that require access to information systems affected during this emergency plan		
2. Establish measures to ensure only authorized persons can gain access to information assets.		
3. Document the supporting systems and resources (for instance authentication services or network services) needed to ensure confidentiality for your network assets in your emergency plan.		
4. Create a plan to ensure any information systems created temporarily during this emergency are physically secure and establishes control to limit general physical access.		

Integrity

Action	Completed?	Documentation Location
1. Document a plan to recreate business critical data resources for use during the emergency plan including necessary infrastructure and hardware requirements,		

2. Develop and document a plan and process to merge any modified business critical data once the emergency plan is no longer in effect which ensures changes are maintained during and after the emergency.		
3. Identify and document any specialized or required tools needed to transfer or share your business critical data assets. Ensure these requirements met on any secondary or emergency systems you are utilizing during this emergency plan.		
4. Develop and document process to ensure that data assets are not overwritten or corrupted by any process that would prevent the effective restoration of services and integration of data assets changed once the emergency plan is no longer in effect?		
5. Identify and document any regulatory compliance requirements (i.e. HIPAA, FERPA, etc.) documented and applied to the contingency operational environment.		

Availability

Action	Completed?	Documentation Location
1. Document the information systems necessary for your unit to continue modified operations during the crisis. Identify any hardware and software dependencies and document processes to restore limited critical services and access to your staff.		
2. Document a plan to ensure that users or services can access any critical systems during this emergency. Creator or document the process is to transfer access to any emergency systems and to revert back to the original systems once the emergency plan is no longer in effect.		
3. Document a plan to provide similar disaster recovery and power redundancy to maintain availability of any information assets established on an emergency basis during the execution of this emergency plan.		