IT Continuity Checklist

This checklist will help guide your actions in protecting critical IT and telecommunications equipment. It includes a list of recommended tasks to be completed during the planning phase, well ahead of a disaster. Customize the tasks to fit the needs of your organization.

Tasks	Initial when complete
Perform security risk assessments around specific threats including virus protection, intrusion detection, hacker prevention and network events. If applicable, work with IT provider to evaluate the likelihood of events and obtain suggestions for mitigating impacts and threats.	
Determine communications hardware needed to stay in communication during an event, including satellite phones and walkie-talkies and work with the **Business Continuity Chief** to approve purchase.	
Ensure that all hardware to support communications with staff is in working order. Coordinate with the **Business Continuity Chief**.	
Add information about hardware and software and warranties to the *IT Equipment Inventory Worksheet* and send to the **Business Continuity Chief**.	
If you work with outside IT vendors, clarify which services will be available during a disaster.	
Discuss options for storing equipment off-site with the **Business Continuity Chief**.	
Set up cloud storage for offsite access to vital records.	
Ensure senior staff have access from remote locations, including home broadband, phone, VPN for security. Coordinate with the **Human Resources Team Leader** to ensure access is included in working-from-home policies.	
Determine the effectiveness of your data backup and recovery policies and procedures. Perform backup at regular intervals, daily, weekly or monthly.	
Notes	