

GREATER COLUMBIA BEHAVIORAL HEALTH Policies and Procedures

Category: Privacy and Security
Approved On: 03/27/2003
Approved By: The Board of Directors
Revised: 00/00/00
Effective Date: 15 days from approval/ the last revision

No: PS616.00

Title: Information Systems Security Checklist: Onsite Inspection

The Information Systems Security Checklist: Onsite Inspection is attached.



**Greater Columbia
Behavioral Health**

Information Systems Security Checklist

On-Site Inspection

Information Systems Security Checklist

On-Site Inspection

Organization:	
Site Location:	
Review Date:	
Staff:	

ITEM	YES	NO
• FACILITIES, EQUIPMENT, AND COMMUNICATIONS		
<ul style="list-style-type: none"> • Does this location have any of the following equipment on site? <ul style="list-style-type: none"> <input type="checkbox"/> Server(s) <input type="checkbox"/> Hub/Switch(s) <input type="checkbox"/> Router(s) <input type="checkbox"/> Firewall appliance(s) <input type="checkbox"/> Modem(s) <input type="checkbox"/> Backup device(s) <input type="checkbox"/> Personal Computer(s) <input type="checkbox"/> Mobile devices (PDAs, etc.) <input type="checkbox"/> Printer(s) <input type="checkbox"/> Fax Machine(s) <input type="checkbox"/> Telecommunication hub/controller(s) <input type="checkbox"/> Software media (CDs, diskettes, etc.) <input type="checkbox"/> Other: _____ <input type="checkbox"/> Other: _____ <input type="checkbox"/> Other: _____ <input type="checkbox"/> Other: _____ <input type="checkbox"/> Other: _____ 		
<ul style="list-style-type: none"> • Is there is written inventory of the above listed equipment? 		
<ul style="list-style-type: none"> • If yes, is the inventory on site? 		
<ul style="list-style-type: none"> • Is there a sign-out procedure/log for removal of equipment? 		
<ul style="list-style-type: none"> • If yes, does the log contain: <ul style="list-style-type: none"> <input type="checkbox"/> Staff name 		

ITEM	YES	NO
<input type="checkbox"/> Staff department <input type="checkbox"/> Reason for removal <input type="checkbox"/> Date of removal <input type="checkbox"/> Date of return <input type="checkbox"/> Supervisor signature		
<ul style="list-style-type: none"> Is the equipment tagged? (View a sample for tags) 		
<ul style="list-style-type: none"> Is the server room on a top or bottom floor? 		
<ul style="list-style-type: none"> Does the server room have windows? 		
<ul style="list-style-type: none"> If yes, are the windows: <ul style="list-style-type: none"> <input type="checkbox"/> Plastic <input type="checkbox"/> Shatterproof <input type="checkbox"/> Bulletproof 		
<ul style="list-style-type: none"> Is there a UPS system(s) to provide temporary power to servers and other critical workstations? If yes, indicate the average time provided by the UPS: <ul style="list-style-type: none"> <input type="checkbox"/> 15 minutes <input type="checkbox"/> 30 minutes <input type="checkbox"/> 1 hour <input type="checkbox"/> 4 hours <input type="checkbox"/> 8 hours <input type="checkbox"/> Indefinitely 		
<ul style="list-style-type: none"> Is a backup generator system used? 		
<ul style="list-style-type: none"> <ul style="list-style-type: none"> If yes, has the generator been inspected and approved in the last 3 months? 		
<ul style="list-style-type: none"> <ul style="list-style-type: none"> Is there a documented schedule and logs for generator testing? 		
<ul style="list-style-type: none"> <ul style="list-style-type: none"> Is there enough fuel on site for 3 days of operation? 		
<ul style="list-style-type: none"> Does the UPS system perform automatic computer backup and shutdown? 		
<ul style="list-style-type: none"> Is there a power failure detection device that will notify a commercial alarm company? 		
<ul style="list-style-type: none"> Does the alarm company have a current priority list of names and telephone numbers to call to notify someone in case of a problem? 		
<ul style="list-style-type: none"> Are there posted procedures for shutting down any hardware that is not essential to the system operation? 		
<ul style="list-style-type: none"> Is there a cellular phone charged and ready? 		
<ul style="list-style-type: none"> Is there a battery-operated radio available? 		
<ul style="list-style-type: none"> Is there a posted procedure designating which computer system should be turned off when a warning sounds? 		
<ul style="list-style-type: none"> Is there a posted procedure for storage of backup media when a warning sounds? 		
<ul style="list-style-type: none"> Do all PCs have surge protectors? 		

ITEM	YES	NO
• Is there a water detection device that will turn off the system and notify a commercial alarm company?		
• Does the alarm company have a current priority list of names and telephone numbers to call to notify someone in case of a problem?		
• Do main server areas have fireproof access doors and nonflammable walls, ceiling and floors?		
• If staff are present, does the extinguisher system turn on automatically after 30 seconds?		
• If staff are not present, does the extinguisher system turn on automatically immediately?		
• Is there a smoke detection device that will notify a commercial alarm company?		
• Does the alarm company have a current priority list of names and telephone numbers to call to notify someone in case of a problem?		
• Are computer operations located in a separate building?		
• If yes, is this building located away from the perimeter?		
• Does the ground floor have windows?		
• If yes, are the windows bullet-proof?		
• Are entryway doors (to server room) constructed of strong fireproof steel with secure locks?		
<ul style="list-style-type: none"> • Is a personal identification system used before staff access is allowed? If yes, indicate type: <ul style="list-style-type: none"> <input type="checkbox"/> Key card <input type="checkbox"/> Key pad <input type="checkbox"/> Biometric device <input type="checkbox"/> Key <input type="checkbox"/> Sentry <input type="checkbox"/> Double door gateway 		
• Is there a separate rest room/staff lounge?		
• Does policy prohibit consumption of food and beverages outside of staff lounge(s)?		
• SITE DATA AND PRIVACY PROTECTION		
• Is there a documented data backup procedure located on site?		
<ul style="list-style-type: none"> • If yes, does the procedure address: <ul style="list-style-type: none"> <input type="checkbox"/> Media type <input type="checkbox"/> Media rotation schedule <input type="checkbox"/> Off-site storage <input type="checkbox"/> Periodic testing <input type="checkbox"/> Personnel responsibilities including backup staff <input type="checkbox"/> Activity logs <input type="checkbox"/> Server and local PCs schedules 		
• Is a fireproof safe(s) used for storing backed-up data and software?		

ITEM	YES	NO
<ul style="list-style-type: none"> If yes, is the safe(s) in a different room than the server(s)? 		
<ul style="list-style-type: none"> Is there a sign-in sheet/mechanism for admission and tracking of non-staff personnel (consultants, technicians, etc.)? 		
<ul style="list-style-type: none"> Are any passwords displayed in public view? 		
<ul style="list-style-type: none"> Is there a client sign-in sheet? 		
<ul style="list-style-type: none"> Are computers/workstations visible from client areas? 		
<ul style="list-style-type: none"> Are there document shredding capabilities and procedures at this location? 	•	•
<ul style="list-style-type: none"> Does this location take preventative measures to ensure that unauthorized persons are prevented from accessing others' health information? (Hint: Look for computer screens masks, password-protected screensavers, and paper records left unattended.) 	•	•
<ul style="list-style-type: none"> Does this location maintain a process to ensure that all health information is appropriately labeled? (Look at all media, including backup tapes, diskettes, output devices and forms.) 	•	•
<ul style="list-style-type: none"> Does this location take appropriate measures to prevent end-users from bypassing the organization's security mechanisms? (Look for sharing of passwords, temporary badges, unauthorized health information storage locations (unlocked desks).) 	•	•
<ul style="list-style-type: none"> Does this location keep a record of breaches and how they were handled? 	•	•
<ul style="list-style-type: none"> Does this location maintain records that document repairs, or modifications to the facility (doors, locks, security systems)? 	•	•
<ul style="list-style-type: none"> Does this location have a central reception/security desk that verifies access privileges prior to granting access to the facility that contains or can access protected health information? 	•	•
<ul style="list-style-type: none"> If appropriate, does this location maintain a visitor log, to include a positive identification check (e.g., a photo ID)? 	•	•
<ul style="list-style-type: none"> Does this location have a written policy on escorted and unescorted visitor requirements? 	•	•
<ul style="list-style-type: none"> DISASTER PROTECTION AND BUSINESS CONTINUITY 		
<ul style="list-style-type: none"> Is there a copy of the agency Disaster/Business Continuity Plan on site? 		
<ul style="list-style-type: none"> Are staff familiar with roles and responsibilities under the Disaster/Business Continuity Plan? (Question random staff) 		
<ul style="list-style-type: none"> Does this location maintain a list of business critical forms? 		
<ul style="list-style-type: none"> Is there a store of business-critical forms for use in an emergency? 		

ITEM	YES	NO
<ul style="list-style-type: none"> • Does this location maintain the following: <ul style="list-style-type: none"> <input type="checkbox"/> Copies of critical reference manuals <input type="checkbox"/> Contact information - personnel, hardware/software vendors, utilities, etc.? <input type="checkbox"/> Copies of business critical procedures? <input type="checkbox"/> Copies of procedures to process paper transactions (e.g., manual procedures) of business critical functions? <input type="checkbox"/> A list of equipment required for processing business critical functions? <input type="checkbox"/> A list of personnel required for supporting the business critical functions? <input type="checkbox"/> A list of services required for supporting business critical processes - phone, electricity, mail, etc.? <input type="checkbox"/> A list of all communications required for supporting business critical functions? <input type="checkbox"/> The emergency notification process and responsibilities? <input type="checkbox"/> A list of hardcopy and local backup strategies for business critical functions? <input type="checkbox"/> A list of key vendor information (name, phone numbers, product and serial numbers) to support business critical functions? <input type="checkbox"/> A list of necessary resources to support the recovery mode? <input type="checkbox"/> Provisions for all human elements required to support the business critical functions - who, what, where, contact information? <input type="checkbox"/> The necessary business function support team composition (functional and technical members) including skill set match, training and testing capabilities? <input type="checkbox"/> Procedures and policies regarding the authorization to initiate contingency operations and resume normal operations? <input type="checkbox"/> Policies and procedures for voice communications to support critical business functions especially as they pertain to Business Continuity Plans? <input type="checkbox"/> Procedures and policies for returning to normal operations? <input type="checkbox"/> Public relations and media interaction guidelines? <input type="checkbox"/> customer interface procedures been defined for the Emergency Mode Operations Plan? 	•	•
• Has this location tested the Disaster Recovery/Business Continuity procedures?	•	•
• Does this location use virus scanning software on all computer systems?	•	•
• Does the virus scanning software automatically download and install new anti-virus software in a timely manner?	•	•
• Does this location scan files and email attachments for virus at the network perimeter (i.e. at the Internet firewall and other network access points)?	•	•
• Does the virus policy at this location restrict users from downloading and installing unapproved software?	•	•
• Does your virus policy at this location restrict users from opening e-mail attachments from unknown sources?	•	•