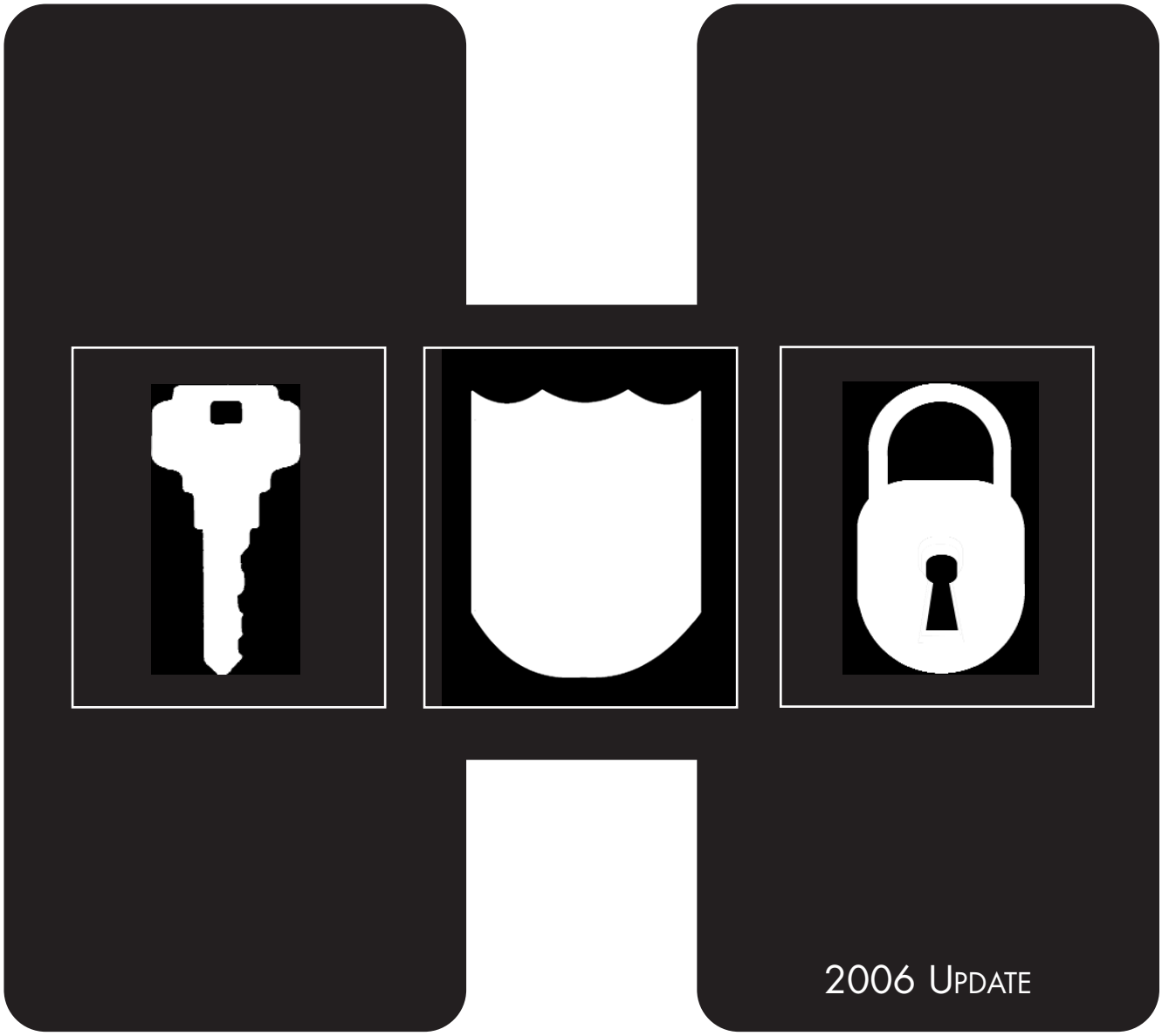
EMERGENCY PREPAREDNESS

HEALTHCARE SECURITY



READINESS ASSESSMENT TOOL

This resource has been produced through a grant supplied by the New Jersey Department of Health and Senior Services.

NJHA
NEW JERSEY HOSPITAL ASSOCIATION

NEW JERSEY DEPARTMENT OF HEALTH AND SENIOR SERVICES

EMERGENCY PREPAREDNESS

INTRODUCTION

At the direction of the Department of Homeland Security, the Attorney General's Office is conducting security audits of hospitals that focus on critical infrastructure. Healthcare is one of 20 critical infrastructure sectors where audited facilities must meet four criteria.

These criteria are:

- Conduct a Hazard Vulnerability Assessment
- Identify gaps through the assessment
- Develop a Corrective Plan of Action
- Have an Emergency Response Plan

When audits of hospital security were first discussed, the Department of Health and Senior Services (DHSS) intended to use NJHA's Security Readiness Assessment Tool. NJHA's concern was that the document reflected all possible security measures that hospitals could undertake without consideration of risk, financial resources or feasibility. In response to this concern, NJHA was given the opportunity by DHSS to establish security "practices" and will evaluate hospitals only in relation to the recommended actions reflected under Basic Practices. As not all hospitals may meet the criteria reflected in Intermediate and Advanced Practices, NJHA expects that most hospitals will work toward achieving higher levels of security over time and with sufficient financial resources.

To develop this approach to hospital security audits, NJHA's Emergency Preparedness staff and members of the Security Subcommittee of the Emergency Preparedness Task Force reviewed guidelines contained within the Hospital Security Readiness Assessment Tool, the color-coded Threat Level Guidelines, and other materials prepared by the state's Domestic Security Task Force Healthcare Infrastructure Advisory Committee (HIAC). The results of this review are contained in the attached document.

In 2006, the tool was reviewed by the Security Committee and NJHA staff to ensure its applicabillity to continuing care facilities. NJHA recommends that you review the guidelines, identify where there may be gaps and focus on those particular areas in your corrective plan of action.

NJHA extends its appreciation to the members of the Security Subcommittee and the hours that they committed to providing guidance to healthcare facilities throughout the state. The Joint Commission on Accreditation of Healthcare Organizations has accepted this tool into it's Good Practices Data Base to acknowledge the documents value in assuring compliance with the Joint Commission standards and improving safety and quality of services provided. The letter from Joint Commission Resources is on the following page.

Joint Commission
RESOURCES

Headquarters
1515 West 22nd Street
Suite 1300W
Oak Brook, Illinois 60523
Voice: 630-268-7400
Fax: 630-268-7405

Branch Offices
13, Chemin du Levant
Immeuble JB SAY
F-01210 Ferney-Voltaire
France
Voice: +33 (0)4 50 42 60 82
Fax: +33 (0)4 50 42 48 82

Via Beatrice d'Este, 20 20100
Milano
C.F. e P.I. 04390030965
Italy
Voice: 02 890 75 940
Fax: 02 890 75 941

http://www.jcrinc.com

An Affiliate of the Joint Commission on Accreditation of Healthcare Organizations

October 4, 2005

Diane Anderson
New Jersey Hospital Association
760 Alexander Road
Princeton, New Jersey 08543

Dear Ms. Anderson:

This letter is to inform you and your organization that your example, "Emergency Preparedness Hospital Security Readiness Assessment Tool" was accepted into Joint Commission Resources' Good Practices Database for Hospitals. Congratulations!

The Good Practices Database for Hospitals contains good practice examples of survey compliance from Joint Commission-accredited organizations that are used in complying with Joint Commission standards and improving the safety and quality of services provided. Every example is rigorously reviewed by Joint Commission standards experts to assure compliance with standards, clinical accuracy, and overall usefulness.

I look forward to posting your good practice example so it can be available to others!

Sincerely,

Jennifer McDonald

Jennifer McDonald
Manager, Good Practices Database
Joint Commission Resources

NJHA
NEW JERSEY HOSPITAL ASSOCIATION

EMERGENCY PREPAREDNESS

TABLE OF CONTENTS

NJHA
NEW JERSEY HOSPITAL ASSOCIATION

EMERGENCY PREPAREDNESS

Basic Practices

Basic practices represent the level of security that facilities should have attained already or be in the process of implementing based on regulatory requirements, the Infrastructure Advisory Committee Healthcare Industry Sector Security Assessment and Best Practices Report, and the Emergency Preparedness Healthcare Security Readiness Assessment Tool.

A. General	Yes	No	If No, Implementation Date
1. There is a written policy identifying an individual, designated by leadership, to coordinate the development, implementation and monitoring of Security Management activities.			
2. There is a current hazard vulnerability analysis (HVA) that is reviewed/revised at least annually.			
3. There is a plan to improve those areas of the HVA that the facility has identified as requiring improvement.			
4. There is evidence of proactive risk assessments that evaluate the potential adverse impact of the external environment on the security of patients, visitors and staff.			
5. There is evidence that protocols are developed and implemented to minimize the impact of the risks identified through risk assessments.			
6. There is a system in place to alert all staff to the current Department of Homeland Security (DHS) threat level.			
7. There is a clear explanation provided to staff regarding what the DHS threat level means and the appropriate action(s) to be taken.			
8. There are protocols in place defining steps to be taken at heightened threat levels.			
9. There are protocols in place and staff is trained regarding protocols for handling suspicious packages and/or mail.			
10. There are protocols in place for employees to report suspicious activities.			

BASIC PRACTICES

A. GENERAL CONTINUED	Yes	No	If No, Implementation Date
11. There are protocols in place regarding internal emergency or security threat communications within the organization and with local law enforcement.			
12. There are protocols in place outlining security incident response and reporting procedures.			
13. There is evidence that security codes and policies are readily accessible, 24/7, in every department (e.g. posted in employee areas).			
14. There is a forensic policy in place.			
15. There is a protocol to address theft of or missing narcotics.			
16. There is evidence that security plans exist and are re-assessed at regular intervals.			
17. There are emergency telephone numbers for police, fire, health, OEM and state hotlines posted prominently in areas deemed appropriate (i.e. ED, security, etc.).			
18. If the facility operates a closed circuit TV security system, the following exist:			
a. A protocol to address covert camera monitoring			
b. Monitoring of high-risk areas			
c. Recording capabilities			
d. Support by emergency power			

BASIC PRACTICES

B. SECURITY STAFFING	Yes	No	If No, Implementation Date
1. There is pre-employment screening for security personnel that includes criminal background checks, if indicated by facility policy.			
2. There is an emergency security staffing plan that includes protocols for staff recall, employee travel, vacation and leave cancellations.			
3. There is a protocol in place assigning personnel at critical facilities to assist with security duties (e.g. monitoring personnel entering the facility, checking vehicles entering the facility, patrolling the area regularly, etc.).			
4. There is a protocol in place to shut down facilities and operations impacted by security emergencies in accordance with contingency plans.			
5. There is a protocol in place to reduce staffing at high-risk facilities to lowest possible levels or shut them down entirely.			
6. There is evidence that when determining security staffing, the following is considered:			
a. Security staffing levels should not be based solely on square footage, but should consider crime rates, hazard vulnerability analysis, overall value of assets, special services required, levels of enforcement and community concerns.			

BASIC PRACTICES

C. SECURITY RESPONSE	Yes	No	If No, Implementation Date
1. There are protocols in place regarding:			
a. Prosecution of criminal offenses against the organization;			
b. Governance of security response to staff, patients and visitors;			
c. General response protocols for security staff that define their authority.			
2. There are job action sheets for the security department outlining security staff roles in the facility's Incident Command System (ICS) and staff is trained accordingly.			
3. There are protocols to routinely check existing security measures such as fencing, locks, camera surveillance, etc. to assure they are in proper working order.			
4. There are protocols for infant security and incident response.			
5. There are protocols in place to assure security officers periodically check perimeter fencing and critical facilities while staying in communication with on-site personnel via two-way radio.			
6. There are measures to identify areas where explosive devices could be hidden.			
7. There are security protocols that address handling the media and/or VIPS.			
8. There are protocols in place that prohibit radio conversations regarding sensitive topics.			

BASIC PRACTICES

D. IDENTIFICATION	Yes	No	If No, Implementation Date
1. There is evidence that identification procedures for visitors, vendors and contractors are in place and include:			
a. Visitor badge/pass that identifies where visitors, vendors and contractors may travel within the facility.			
2. There is evidence that identification procedures for employees, physicians and volunteers are in place and include:			
a. ID cards that include a photo, wearer's name, department and title or credentials (i.e. MD, RN);			
b. An enforcement procedure to ensure ID is worn at all times. Exceptions are when wearing the ID would put the employee at risk for injury, in which case the ID must be carried;			
c. Procedures employees follow when the arrive at facility without their ID;			
d. Procedures for lost/stolen ID;			
e. Procedures for return of ID upon separation from employment;			
f. Restriction of access to sensitive areas defined by the facility (e.g. mother/infant, pharmacy, lab);			
g. Protocol addressing access restriction for terminated employees;			
h. Protocol requiring that resigned or terminated employees turn in equipment, access cards and keys at time of termination/resignation;			
i. Protocol identifying who is authorized to create identification and addresses the handling and storage of blank and terminated identification.			
3. There is a protocol in place to account for all employees during a crisis.			

BASIC PRACTICES

E. SEARCHES	Yes	No	If No, Implementation Date
1. There is a protocol in place regarding:			
a. The inspection and control of facility security vehicles;			
b. Searches of suspicious packages and persons. Protocols should define clearly what characterizes a person/package as suspicious;			
c. Searches of employee packages or lockers;			
d. The inspection of all vehicles entering critical facilities, including cargo areas, undercarriage, glove compartments and other areas where dangerous items could be concealed;			
e. The inspection of all packages carried by visitors - including the posting of signs informing individuals that their persons/package(s) may be searched at the facility's discretion.			

BASIC PRACTICES

F. TRAINING	Yes	No	If No, Implementation Date
1. There is documentation that indicates that all new security employees must receive new employee and departmental orientation.			
2. There is evidence of pertinent annual training programs for security staff (e.g. handcuffs, use of physical force, weapons, aggressive behavior, physical security).			
3. There is evidence that security staff receive regular training, which includes:			
a. Threat assessments;			
b. National threat levels;			
c. WMD awareness as well as task specific training based on roles in an emergency response (e.g. PPE training if they are required to wear equipments in the event of biological release or if they participate in decontamination);			
d. Specific responsibilities related to emergency management;			
e. Security policies, procedures and appropriate responses.			
4. There is evidence that security staff is evaluated for competency.			
5. There is evidence that security staff exercise/drill based on their role in emergency response plans (e.g. fire, bomb threats, biological threats, suspicious mail, evacuation, employee recall lists).			
6. There is evidence that security staff have tested their role in emergency response plans with local law enforcement, bomb squad, fire department, etc.			
7. A security orientation must be provided to all new employees, volunteers, etc.			
8. There is evidence that senior security staff members mentor new security officers.			
9. There is training in place for mailroom and receiving staff to identify suspicious packages.			

BASIC PRACTICES

G. ACCESS	Yes	No	If No, Implementation Date
VISITORS			
1. Protocols are in place to limit or restrict the number of visitors to patients in inpatient areas. Protocol allows for case-by-case exceptions.			
2. Protocols are in place that indicate the facility, during increased threat levels, considers using only one entrance for all visitors, and ensures that visitor protocols are strictly enforced.			
3. Protocols are in place for refusal of access to people who do not have positive identification or do not have a legitimate need to enter the site.			
4. Protocols are in place to identify the owners of all vehicles at critical facilities and remove all vehicles whose owners have not been identified.			
DELIVERIES			
1. There are protocols regarding deliveries during and after normal working hours.			
2. There are protocols in place regarding appropriate limitation or control of access to the loading dock.			
3. There is evidence that the facility has assessed the impact of travel restrictions on deliveries.			
EMPLOYEES			
1. There are protocols regarding key issuance and control.			
2. Procedures are in place to terminate access to voice mail, e-mail and health information and patient accounting systems upon employee termination.			
3. There is a protocol for transporting staff in an emergency.			
4. There is evidence that staff have been educated regarding travel ban restrictions established by the state police and are aware that ID is required if traveling.			

BASIC PRACTICES

G. ACCESS CONTINUED	Yes	No	If No, Implementation Date
RESTRICTING ACCESS CONTINUED			
1. There is evidence that signs are posted at the entrance of restricted or sensitive areas indicating "Unauthorized Personnel Not Permitted" or "Authorized Personnel Only."			
2. There is evidence that the following have been evaluated for security risks: Nuclear Medicine, Interventional Radiology, Microbiology Lab, Power Plant, Water System, Pressurized Gasses, Blood Supply.			
3. There is evidence of a security protocol that addresses vehicular access to emergency care areas.			
4. Protocols are in place and tested to rapidly shut down access to portions of the entire facility.			
5. Protocols are in place indicating when to limit the number of facility access points.			
6. Protocols identify appropriate times or events when site ingress and egress points are reduced to an absolute minimum.			
7. There is evidence of an access control protocol for emergencies.			
8. Protocols exist to, in coordination with law enforcement, extend the facility perimeter in an emergency.			
9. Protocols exist to, in coordination with law enforcement, distance vehicle checkpoints in an emergency.			
10. Protocols are in place to ensure that employees do not prop access control points (doors/windows) open.			
11. Protocols are in place that dictate when to request assistance from local law enforcement agencies in securing the facility and access.			
12. There is evidence the facility has evaluated transportation routes and parking areas to determine whether the routes allow contact with facility-defined sensitive areas. Barriers are erected to block access as appropriate to the situation			

BASIC PRACTICES

G. ACCESS CONTINUED	Yes	No	If No, Implementation Date
RESTRICTING ACCESS CONTINUED			
13. There are protocols for crowd and traffic control in an emergency.			
14. There is evidence that the facility has created an emergency traffic plan with local law enforcement.			
15. There is evidence that medical gases are secured.			
16. Protocols are in place to identify locations and determine safe distances of US Postal and other delivery mailboxes.			
17. Protocols are in place to secure all emergency generators and identify areas served.			
18. Protocols are in place to identify and secure air handling units, air intake units, their location and areas served.			

BASIC PRACTICES

H. CYBER SECURITY	Yes	No	If No, Implementation Date
1. There is evidence that the organization has a designated individual to coordinate the cyber security program.			
2. There are cyber security standards and guidelines that include:			
a. A data classification scheme that requires specific security measures based on the criticality of data and the risks that unauthorized access or modification would pose. The more critical the data, the more stringent security precautions should be employed.			
b. Restricting access to information that could aid terrorists.			
c. An asset classification scheme that requires specific security measures based on the risk of unauthorized access or damage to the asset or property.			
3. There is regular monitoring of these standards for compliance.			
4. There are unique user IDs and passwords and periodic password changes are required.			
5. There are limited users with unrestricted or superuser privileges.			
6. There are monitored processes for removing terminated users.			
7. There is a process to modify access controls when users change jobs.			
8. There are secure measures (VPN, SSL, etc.) for employees or contractors with connectivity to the network via the Internet.			
9. There are firewalls to restrict access from the Internet.			
10. There is monitoring for unauthorized access points (modems, access points (wireless), remote control software).			
11. There are procedures to follow when an unauthorized attempt occurs that includes reporting, damage assessment, remediation and follow up.			

BASIC PRACTICES

H. CYBER SECURITY CONT'D.	Yes	No	If No, Implementation Date
12. There are hardening procedures (limit computer services and functionality to that which is needed) used by system and network administrators for critical computer systems and processes.			
13. There are security patches applied within reasonable time-frames.			
14. There is anti-virus software on network-connected systems with timely updates to virus definition files, where appropriate.			
15. There are browser settings that detect and alert users for unauthorized access to users' machines.			
16. If the organization has web-based mission critical applications, the data and the ability to process transactions is fully protected from direct access on the Web site.			
17. There are regular backups performed and off-site storage for mission critical backups.			
18. There is an information assurance program to monitor compliance with security policies.			
19. There are periodic computer vulnerability assessments performed on internal systems and for Internet connectivity as defined by HIPAA or subsequent to changes in infrastructure.			
20. There is assurance that outsourced service providers comply with the organization's security policies, standards and procedures for access to critical systems and processes. There is a signed business associates' agreement for every outsourced service provider.			

EMERGENCY PREPAREDNESS

INTERMEDIATE PRACTICES

Intermediate Practices represent policies, procedures and/or protocols that facilities may wish to ensure are in place to comply with NJDHSS' increased level of security preparedness. *(Intermediate Practices reflected in bold and italics are measures that have been added to the practices you were provided at the Basic level. If you have followed the previous recommendations, you need only address these new directives).*

A. GENERAL	Yes	No	If No, Implementation Date
1. There is a written policy identifying an individual, designated by leadership, to coordinate the development, implementation and monitoring of Security Management activities.			
2. There is a current hazard vulnerability analysis (HVA) that is reviewed/revised at least annually, or at regular intervals.			
3. There is evidence that there is a plan to improve those areas of the HVA that the facility has identified as requiring improvement.			
4. There is evidence of proactive risk assessments that evaluate the potential adverse impact of the external environment on the security of patients, visitors and staff.			
5. There is evidence that protocols are developed and implemented to minimize the impact of the risks identified through risk assessments.			
6. There is a system in place to alert all staff to the current Department of Homeland Security (DHS) threat level.			
7. There is a clear explanation provided to staff regarding what the DHS threat level means and the appropriate action(s) to be taken.			
8. There are protocols in place defining steps to be taken at heightened threat levels.			
9. There are protocols in place and staff is trained regarding protocols for handling suspicious packages and/or mail.			
10. There are protocols in place for employees to report suspicious activities.			

INTERMEDIATE PRACTICES

A. GENERAL CONTINUED	Yes	No	If No, Implementation Date
11. There are protocols in place regarding internal emergency or security threat communications within the organization and with local law enforcement.			
12. There are protocols in place outlining security incident response and reporting procedures.			
13. There is evidence that security codes and policies are readily accessible, 24/7, in every department (e.g. posted in employee areas).			
14. There is a forensic policy in place.			
15. There is a protocol to address theft of or missing narcotics.			
16. There is evidence that security plans exist and are re-assessed at regular intervals.			
17. There are emergency telephone numbers for police, fire, health, OEM and state hotlines posted prominently in areas deemed appropriate (i.e. ED, Security, etc.).			
18. If the facility operates a closed circuit TV security system, the following exist:			
a. A protocol to address covert camera monitoring			
b. Monitoring of high risk areas			
c. Recording capabilities			
d. Support by emergency power			
19. There is evidence that local law enforcement was involved in the preparation of the facilities hazard vulnerability analysis.			
20. There are protocols in place at specific threat levels to review or evaluate the need for:			
a. Operations plans;			
b. Personnel assignments;			

INTERMEDIATE PRACTICES

A. GENERAL CONTINUED	Yes	No	If No, Implementation Date
c. Logistical requirements;			
d. 24/7 security of critical facilities using either contract or company personnel;			
e. Restriction of access to essential personnel only at critical facilities;			
f. Protocols governing the use of force and pursuit (as appropriate) with security personnel.			
21. There are protocols, if applicable, that include advising employees working alone at remote locations to check in with security periodically.			
22. There is evidence that staff is advised not to speak to outsiders concerning the facility or its operation and to report the presence of unknown suspicious persons, vehicles and/or mail.			
23. There are procedures in place to ensure:			
a. Appropriate employees are aware of terror alert advisories issued by the New Jersey Office of Counterterrorism (OCT) and other agencies;			
b. The implementation of appropriate measures.			
24. There is documented monitoring of compliance with security codes through testing. (i.e. lock-down / bomb threat, etc.).			
25. There is evidence that the organization has a copy of the local OEM's emergency plans or documented proof of request.			
26. There are protocols in place to hold managers accountable for an employee's lack of compliance with or violation of security protocols.			

INTERMEDIATE PRACTICES

A. GENERAL CONTINUED	Yes	No	If No, Implementation Date
27. There are protocols in place to advise local law enforcement of any upgraded security measures resulting from an elevation of the threat level, that would impact their ability to respond to your facility.			
28. There are protocols in place to re-evaluate the surrounding area to determine if activities near a critical facility could create hazards that could affect the facility..			
29. There are protocols in place that identify the level at which the organization will implement procedures requiring facility managers to periodically provide the status of security measures implemented.			

INTERMEDIATE PRACTICES

B. SECURITY STAFFING	Yes	No	If No, Implementation Date
1. There is pre-employment screening for security personnel that includes criminal background checks, if indicated by facility policy.			
2. There is an emergency security-staffing plan that includes protocols for staff recall, employee travel, vacation and leave cancellations.			
3. There is a protocol in place assigning personnel at critical facilities to assist with security duties (e.g. monitoring personnel entering the facility, checking vehicles entering the facility, patrolling the area regularly, etc.).			
4. There is a protocol in place to shut down facilities and operations impacted by security emergencies in accordance with contingency plans.			
5. There is a protocol in place to reduce staffing at high-risk facilities to lowest possible levels or shut them down entirely.			
6. There is evidence that when determining security staffing, the following is considered:			
a. Security staffing levels should not be based solely on square footage, but should consider crime rates, hazard vulnerability analysis, overall value of assets, special services required, levels of enforcement and community concerns.			

INTERMEDIATE PRACTICES

C. SECURITY RESPONSE	Yes	No	If No, Implementation Date
1. There are protocols in place regarding:			
a. Prosecution of criminal offenses against the organization;			
b. Governance of security response to staff, patients, and visitors;			
c. General response protocols for security staff that define their authority.			
2. There are job action sheets for the security department outlining security staff roles in the facility's Incident Command System (ICS) and staff is trained accordingly.			
3. There are protocols in place to assure security officers periodically check perimeter fencing and critical facilities while staying in communication with on-site personnel via two-way radio.			
4. There are protocols to routinely check existing security measures such as fencing, locks, camera surveillance, etc. to assure they are in proper working order.			
5. There are protocols for infant security and incident response.			
6. There are measures in place at the facility to identify areas where explosive devices could be hidden.			
7. There are security protocols that address handling the media and/or VIPs.			
8. There are protocols in place that prohibit radio conversations regarding sensitive topics.			

INTERMEDIATE PRACTICES

D. IDENTIFICATION	Yes	No	If No, Implementation Date
1. There is evidence that identification procedures for visitors, vendors and contractors are in place and include:			
a. Visitor badge/pass that identifies where visitors, vendors and contractors may travel within the facility.			
2. There is evidence that identification procedures for employees, physicians and volunteers are in place and include:			
a. ID cards that include a photo, wearer's name, department and title or credentials (i.e. MD, RN);			
b. An enforcement procedure to ensure ID is worn at all times. Exceptions are when wearing the ID would put the employee at risk for injury, in which case the ID must be carried;			
c. Procedures employees follow when the arrive at facility without their ID;			
d. Procedures for lost/stolen ID;			
e. Procedures for return of ID upon separation from employment;			
f. Restriction of access to sensitive areas defined by the facility (e.g. mother/infant, pharmacy, lab);			
g. Protocol addressing access restriction for terminated employees;			
h. Protocol requiring that resigned or terminated employees turn in equipment, access cards and keys at time of termination/resignation;			
i. Protocol identifying who is authorized to create identification and addresses the handling and storage of blank and terminated identification.			
3. There is a protocol in place to account for all employees during a crisis.			

INTERMEDIATE PRACTICES

D. IDENTIFICATION CONT'D.	Yes	No	If No, Implementation Date
4. There is evidence that visitors are advised that the badge/pass they receive restricts the areas they may access.			
5. There is evidence that visitors are advised that their pass/badge must be visible at all times.			
6. There is evidence that outpatient identification is different from visitor ID.			
7. There is evidence that vendor badges/ passes are very distinct from all others.			
8. There is evidence that contractor's badges are different from all others. They may be different for daily versus weekly contractors.			
9. There is evidence that visitor identification includes sign-in procedures.			
10. There is evidence that all vendors and/or contractors report to a central area to obtain a pass/badge and indicate where they are going.			
11. Security requires all vendors and/or contractors leave a driver's license at sign-in to be retrieved as they leave the site.			
12. Vendors or contractors that visit on a regular basis have photo ID, the cost of which is covered by the vendor.			
13. There are protocols that address consequences for employees who fail to carry/show ID. Consequences may include:			
a. Supervisors are contacted to authorize staff that attempt to enter without ID;			

INTERMEDIATE PRACTICES

D. IDENTIFICATION CONT'D.	Yes	No	If No, Implementation Date
b. Staff and physicians that do not have ID must sign a log book;			
c. Staff/physicians who refuse to show ID are reported to department head and administration;			
d. After three incidents, staff member must be reported to the department head or administration; and/or,			
e. After three incidents, staff are suspended.			
14. There is evidence that identification procedures for employees, physicians and volunteers include a protocol regarding handling of individuals in areas where they are not authorized.			
15. There is evidence that staff is advised that if visitors are found without a pass/ badge they must be escorted to security.			

INTERMEDIATE PRACTICES

E. SEARCHES	Yes	No	If No, Implementation Date
1. There is a protocol in place regarding:			
a. The inspection and control of facility security vehicles;			
b. Searches of suspicious packages and persons. Protocols should clearly define what characterizes a person/package as suspicious;			
c. Searches of employee packages or lockers;			
d. The inspection of all vehicles entering critical facilities, including cargo areas, undercarriage, glove compartments and other areas where dangerous items could be concealed;			
e. The inspection of all packages carried by visitors - including the posting of signs informing individuals that their persons/package(s) may be searched at the facilities discretion.			

INTERMEDIATE PRACTICES

F. TRAINING	Yes	No	If No, Implementation Date
1. There is documentation that indicates that all new security employees have received new employee and departmental orientation.			
2. There is evidence of pertinent annual training programs for security staff (e.g. handcuffs, use of physical force, weapons, aggressive behavior, physical security).			
3. There is evidence that security staff receive regular training, which includes:			
a. Threat assessments;			
b. National threat levels;			
c. WMD awareness as well as task specific training based on their roles in emergency response (e.g. PPE training if they are required to wear equipments in the event of biological release or if they participate in decontamination);			
d. Specific responsibilities related to emergency management;			
e. Security policies, procedures and appropriate responses.			
4. There is evidence that security staff is evaluated for competency.			
5. There is evidence that security staff exercise/drill based on their role in emergency response plans (e.g. fire, bomb threats, biological threats, suspicious mail, evacuation, employee recall lists).			
6. There is evidence that security staff have tested its role in emergency response plans with local law enforcement, bomb squad, fire department, etc.			
7. A security orientation must be provided to all new employees, volunteers, etc.			
8. There is evidence that senior security staff members mentor new security officers.			

INTERMEDIATE PRACTICES

F. TRAINING CONTINUED	Yes	No	If No, Implementation Date
9. There is training in place for mailroom and receiving staff to identify suspicious packages.			
10. There is evidence that training includes searching of packages, patients, visitors and staff.			
11. There is evidence that security staff is trained to inspect vehicles.			
12. There is evidence that security training is developed and based on the recommendations of the International Association of Health Care Safety and Security (IAHSS) programs.			
13. There is documented ongoing security awareness training for every employee. (Suggestion: Could be done at a departmental level.)			

INTERMEDIATE PRACTICES

G. ACCESS	Yes	No	If No, Implementation Date
VISITORS			
1, Protocols are in place to limit or restrict the number of visitors to patients in inpatient areas. Protocol allows for case-by-case exceptions.			
2. Protocols are in place that indicate the facility, during increased threat levels, considers using only one entrance for all visitors, and ensures that visitor protocols are strictly enforced.			
3. Protocols are in place for refusal of access to people who do not have positive identification or do not have a legitimate need to enter the site.			
4. Protocols are in place to identify the owners of all vehicles at critical facilities and remove all vehicles whose owners have not been identified.			
5. There is evidence that the facility requires appropriate departments to report to a central location and escort all vendors to prevent them from wandering (i.e. pharmaceutical vendors are known to wander floor to floor and leave samples).			
6. There is evidence that security staff is notified at least 24 hrs in advance of when contractors will be working in the facility.			
a. For emergency contractor access, security is notified immediately after call is made to request contractor provide emergency assistance.			
7. There are signs posted in the emergency department indicating that the number of visitors will be limited for security or other reasons so that patients and visitors know that staff is not imposing arbitrary limitations on visitors.			

INTERMEDIATE PRACTICES

G. ACCESS CONTINUED	Yes	No	If No, Implementation Date
8. There are signs posted at appropriate locations of the facility noting visiting hours, access requirements, trespassing, etc.			
9. There are signs posted at points of access to instruct contractors/vendors etc. that they must coordinate their access with specific departments, i.e. media with public relations and contractors with maintenance/facilities.			
10. There is evidence that the facility evaluates if and/or when to limit use of public areas and conference facilities by outside organizations.			
11. There is evidence that the facility limits visitation and confirms that every visitor is authorized to be in a critical facility. All unidentified visitors should be escorted while in critical facilities.			
DELIVERIES			
1. There are protocols regarding deliveries during and after normal working hours.			
2. There are protocols in place regarding appropriate limitation or control of access to the loading dock.			
3. There is evidence that the facility has assessed the impact of travel restrictions on deliveries.			
4. There is evidence of monitoring and securing of the dock area via security staff, gates, cameras, etc.			
5. There is evidence that flower deliveries must to be made to one location (i.e. lobby) and require volunteers deliver.			

INTERMEDIATE PRACTICES

G. ACCESS CONTINUED	Yes	No	If No, Implementation Date
DELIVERIES CONTINUED			
6. There is evidence that the facility requires food delivered from the outside be delivered to one specific location and employees must report to that location to pick up.			
7. There is evidence that the facility requires that all packages (i.e. UPS, Fed-Ex) be delivered to one central location and internal delivery made by employees.			
8. There is evidence that the facility allows only emergency deliveries after 4:30 PM, or requires after-hours deliveries go to security.			
EMPLOYEES			
1. There are protocols regarding key issuance and control.			
2. Procedures are in place to terminate access to voice mail, e-mail and health information and patient accounting systems upon employee termination.			
3. There is a protocol for transporting staff in an emergency.			
4. There is evidence that staff has been educated regarding travel ban restrictions established by the state police and are aware that ID is required if traveling.			
5. The following exist, if there is a closed circuit TV system:			
a. Protocol for monitoring by security staff;			
b. Training program for staff operating/monitoring; and,			
c. Protocols for the use and testing of the system.			
6. There are protocols in place for use, response and testing of a panic alarm system, if in use.			

INTERMEDIATE PRACTICES

G. ACCESS CONTINUED	Yes	No	If No, Implementation Date
RESTRICTING ACCESS			
1. There is evidence that signs are posted at the entrance of restricted or sensitive areas indicating "Unauthorized Personnel Not Permitted" or "Authorized Personnel Only."			
2. There is evidence that the following have been evaluated for security risks: Nuclear Medicine, Interventional Radiology, Microbiology Lab, Power Plant, Water System, Pressurized Gasses, Blood Supply.			
3. There is evidence of a security protocol that addresses vehicular access to emergency care areas.			
4. Protocols are in place and tested to rapidly shut down access to portions of the entire facility.			
5. Protocols are in place indicating when to limit the number of facility access points.			
6. Protocols identify appropriate times or events during which to reduce site ingress and egress points to an absolute minimum.			
7. There is evidence of an access control protocol for emergencies.			
8. Protocols exist to, in coordination with law enforcement, extend the building perimeter in an emergency.			
9. Protocols exist to, in coordination with law enforcement, distance vehicle checkpoints in an emergency.			
10. Protocols are in place to ensure that employees do not prop access control points (doors/windows) open.			
11. Protocols are in place to dictate when to request assistance from the local law enforcement agencies in securing the facility and access.			
12. There is evidence the facility has evaluated transportation routes and parking areas to determine whether the routes allow contact with sensitive areas. Barriers are erected to block access as appropriate to the situation.			

INTERMEDIATE PRACTICES

G. ACCESS CONTINUED	Yes	No	If No, Implementation Date
RESTRICTING ACCESS CONTINUED			
13. There are protocols for crowd and traffic control in an emergency.			
14. There is evidence that the facility has created an emergency traffic plan with local law enforcement.			
15. There is evidence that medical gases are secured.			
16. Protocols are in place to identify locations and determine safe distances of US Postal and other delivery mailboxes.			
17. Protocols are in place to secure all emergency generators and identify areas served.			
18. Protocols are in place to identify and secure air handling units, air intake units, their location and areas served.			
19. There are protocols in place to insure access integrity in the event of a power failure, if an electronic access control system is in use.			
20. There is evidence that a rapidly deployable method for blocking all vehicular traffic into and out of a facility is in place.			
21. The following exist, if metal detectors are in use:			
a. Training for staff;			
b. Protocols regarding who will be required to pass through;			
c. Protocols outlining appropriate action if alarm is activated;			
d. Protocols identifying security's response to a person's refusal to pass through metal detector;			
e. A policy identifying security's response to a person's refusal to comply with any part of policy regarding the metal detector;			

INTERMEDIATE PRACTICES

G. ACCESS CONTINUED	Yes	No	If No, Implementation Date
RESTRICTING ACCESS CONTINUED			
f. Policies are in place and staff is trained to respond to weapons or potential weapons brought in by patients, visitors, staff, local law enforcement and prison guards.			
22. The facility has identified when/where to erect barriers to block access to sensitive areas during increased threat levels.			
23. There is evidence that security personnel have coordinated with local law enforcement to gain an understanding of which transportation routes may be blocked during a red threat level.			
a. Determine how traffic will be controlled.			
b. Determine facilities responsibility to provide support to control traffic flow.			
24. There is evidence that the access control system controls access of outpatient areas into the facility.			
25. There is evidence that the facility assures terminations occur only when human resource representatives are present rather than 24/7.			
26. There is evidence that the facility requires that human resources notify security daily on a concurrent basis of all terminations or resignations so that security may restrict access accordingly.			
27. There is evidence that the facility requires that one department be responsible for terminating access to all information/phone systems as well as access to the facility.			
28. There is evidence that the facility uses a standardized form/checklist of steps to be taken for controlling terminated employee access.			

INTERMEDIATE PRACTICES

G. ACCESS CONTINUED	Yes	No	If No, Implementation Date
RESTRICTING ACCESS CONTINUED			
29. There is evidence that the facility assures that all personal, company and contractor vehicles at critical facility sites be secured and parked legally and at a distance from critical areas.			
30. There is evidence that the facility has evaluated and plans to erect more barriers to control direction of traffic flow and protect the facility by strategically positioning heavy company vehicles.			
31. There is evidence that the facility has installed collision barriers as needed, according to a hazard vulnerability analysis.			
32. There are protocols to identify when to verify that all incoming vehicles and people are authorized and that to the extent possible all vehicles, people, mail, packages, brief cases, etc., are checked entering and leaving the site and placards are placed on visiting vehicles indicating they have been checked by security.			

INTERMEDIATE PRACTICES

H. CYBER SECURITY	Yes	No	If No, Implementation Date
1. There is evidence that the organization has a designated individual to coordinate the cyber security program.			
2. There are cyber security standards and guidelines that include:			
a. A data classification scheme that requires specific security measures based on the criticality of data and the risks that unauthorized access or modification would pose. The more critical the data, the more stringent security precautions should be employed.			
b. Restricting access to information that could aid terrorists.			
c. An asset classification scheme that requires specific security measures based on the risk of unauthorized access or damage to the asset or property.			
3. There is regular monitoring of these standards for compliance.			
4. There are unique user IDs and passwords and periodic password changes are required.			
5. There are limited users with unrestricted or superuser privileges.			
6. There are monitored processes for removing terminated users.			
7. There is a process to modify access controls when users change jobs.			
8. There are secure measures (VPN, SSL, etc.) for employees or contractors with connectivity to the network via the Internet.			
9. There are firewalls to restrict access from the Internet.			
10. There is monitoring for unauthorized access points (modems, access points (wireless), remote control software).			
11. There are procedures for what to do when an unauthorized attempt occurs, that includes reporting, damage assessment, remediation and follow up.			

INTERMEDIATE PRACTICES

H. CYBER SECURITY CONT'D.	Yes	No	If No, Implementation Date
12. There are hardening procedures (limit computer services and functionality to that which is needed) used by system and network administrators for critical computer systems and processes.			
13. There are security patches applied within reasonable timeframes.			
14. There is anti-virus software on network-connected systems with timely updates to virus definition files, where appropriate.			
15. There are browser settings that detect and alert users for unauthorized access to users' machines.			
16. If the organization has Web-based mission critical applications, the data and the ability to process transactions is fully protected from direct access on the Web site.			
17. There are regular backups performed and off-site storage for mission critical backups.			
18. There is an information assurance program to monitor compliance with security policies.			
19. There are periodic computer vulnerability assessments performed on internal systems and for Internet connectivity as defined by HIPAA or subsequent to changes in infrastructure.			
20. There is assurance that outsourced service providers comply with the organization's security policies, standards and procedures for access to critical systems and processes. There is a signed business associates' agreement for every outsourced service provider.			
21. There are business continuity/disaster recovery plans for mission critical processes, and they are tested/updated regularly.			
22. Computer, server and telecom rooms, data closets, routers and hubs are secured.			
23. There is evidence that organizations:			
a. Conduct a cyber-security training and awareness program.			

INTERMEDIATE PRACTICES

H. CYBER SECURITY CONT'D.	Yes	No	If No, Implementation Date
b. Participate in professional organizations and liaison with state and federal law enforcement as well as other cyber-security-related agencies to remain aware of security trends and threats.			
c. Test the strength of users' passwords.			
d. Create measures (host-based intrusion detection, access lists, etc.) to detect unauthorized activity on critical servers.			

EMERGENCY PREPAREDNESS

ADVANCED PRACTICES

Advanced Practices represent protocols and/or actions that facilities may wish to put in place to further improve upon security preparedness and achieve the highest level of NJDHSS' increased level of security preparedness. Many of these recommendations may require significant capital expenditures and are presented here for future reference or evaluation only. ***(Advanced Practices highlighted in bold and italics are measures that we have added to the Basic and Intermediate Practices).***

A. GENERAL	Yes	No	If No, Implementation Date
1. There is a written policy identifying an individual, designated by leadership, to coordinate the development, implementation and monitoring of Security Management activities.			
2. There is a current hazard vulnerability analysis (HVA) that is reviewed/revised at least annually, or at regular intervals.			
3. There is evidence that there is a plan to improve those areas of the HVA that the facility has identified as requiring improvement.			
4. There is evidence of proactive risk assessments that evaluate the potential adverse impact of the external environment on the security of patients, visitors and staff.			
5. There is evidence that protocols are developed and implemented to minimize the impact of the risks identified through risk assessments.			
6. There is a system in place to alert all staff to the current Department of Homeland Security (DHS) threat level.			
7. There is a clear explanation provided to staff regarding what the DHS threat level means and the appropriate action(s) to be taken.			
8. There are protocols in place defining steps to be taken at heightened threat levels.			
9. There are protocols in place and staff is trained regarding protocols for handling suspicious packages and/or mail.			
10. There are protocols in place for employees to report suspicious activities.			

ADVANCED PRACTICES

A. GENERAL CONTINUED	Yes	No	If No, Implementation Date
11. There are protocols in place regarding internal emergency or security threat communications within the organization and with local law enforcement.			
12. There are protocols in place outlining security incident response and reporting procedures.			
13. There is evidence that security codes and policies are readily accessible, 24/7, in every department (e.g. posted in employee areas).			
14. There is a forensic policy in place.			
15. There is a protocol in place to address theft of or missing narcotics.			
16. There is evidence that security plans exist and are re-assessed at regular intervals.			
17. There are emergency telephone numbers for police, fire, health, OEM and state hotlines posted prominently in areas deemed appropriate (i.e. ED, security, etc.).			
18. If the facility operates a closed circuit TV security system, the following exist:			
a. A protocol to address covert camera monitoring			
b. Monitoring of high-risk areas			
c. Recording capabilities			
d. Support by emergency power			
19. There is evidence that local law enforcement was involved in the preparation of the facilities hazard vulnerability analysis.			
20. There are protocols in place that indicate the need, at specific threat levels, to review or evaluate the need for:			
a. Operations plans;			
b. Personnel assignments;			

ADVANCED PRACTICES

A. GENERAL CONTINUED	Yes	No	If No, Implementation Date
c. Logistical requirements;			
d. 24/7 security of critical facilities using either contract or company personnel;			
e. Restriction of access to essential personnel only at critical facilities;			
f. Protocols governing the use of force and pursuit (as appropriate) with security personnel.			
21. There are protocols, if applicable, that include advising employees working alone at remote locations to check in with security periodically.			
22. There is evidence that staff is advised not to speak to outsiders concerning the facility or its operation and to report the presence of unknown suspicious persons, vehicles and/or mail.			
23. There are procedures in place to ensure:			
a. Appropriate employees are aware of terror alert advisories issued by the New Jersey Office of Counterterrorism (OCT) and other agencies;			
b. The implementation of appropriate measures.			
24. There is documented monitoring of compliance with security codes through testing. (i.e. lockdown / bomb threat, etc.).			
25. There is evidence that the organization has a copy of the local OEM's emergency plans or documented proof of request.			
26. There are protocols in place to hold managers accountable for an employee's lack of compliance with or violation of security protocols.			
27. There are protocols in place to advise local law enforcement of any upgraded security measures resulting from an elevation of the threat level, that would impact their ability to respond to your facility.			

ADVANCED PRACTICES

A. GENERAL CONTINUED	Yes	No	If No, Implementation Date
28. There are protocols in place to re-evaluate the surrounding area to determine if activities near a critical facility could create hazards that could affect the facility.			
29. There are protocols in place that identify the level at which the organization will implement procedures requiring facility managers to periodically provide the status of security measures implemented.			
30. There is evidence that the facility has participated in the FBI's Security Awareness Program concerning awareness to national security issues.			
31. There is evidence that the facility is utilizing the American Society of Industrial Security's (ASIS) security checklists, peer review audits and other bench marking processes and strategies to continually review and improve security standards, policies and practices.			
32. There is evidence that the facility has implemented a parking plan to:			
a. Move automobiles and other non-stationary items at least 30 yards from critical facilities, particularly buildings and sensitive areas, unless doing so would create a safety hazard or impede other security;			
b. Implement a centralized parking and shuttle-bus service where feasible; and,			
c. Implement increased number and frequency of vehicular campus patrols.			

ADVANCED PRACTICES

B. SECURITY STAFFING	Yes	No	If No, Implementation Date
1. There is pre-employment screening for security personnel that includes criminal background checks, if indicated by facility policy.			
2. There is an emergency security-staffing plan that includes protocols for staff recall, employee travel, vacation and leave cancellations.			
3. There is a protocol in place assigning personnel at critical facilities to assist with security duties. (e.g. monitoring personnel entering the facility, checking vehicles entering the facility, patrolling the area regularly, etc.).			
4. There is a protocol in place to shut down facilities and operations impacted by security emergencies in accordance with contingency plans.			
5. There is a protocol in place to reduce staffing at high-risk facilities to lowest possible levels or shut them down entirely.			
6. There is evidence that when determining security staffing, the following is considered:			
a. Security staffing levels should not be based solely on square footage, but should consider crime rates, hazard vulnerability analysis, overall value of assets, special services required, levels of enforcement and community concerns.			
7. There is 24/7 camera and staff monitoring of main pedestrian entrance.			

ADVANCED PRACTICES

C. SECURITY RESPONSE	Yes	No	If No, Implementation Date
1. There are protocols in place regarding:			
a. Prosecution of criminal offenses against the organization;			
b. Governance of security response to staff, patients and visitors;			
c. General response protocols for security staff that define their authority.			
2. There are job action sheets for the security department outlining security staff roles in the facility's Incident Command System (ICS) and staff is trained accordingly.			
3. There are protocols in place to assure security officers periodically check perimeter fencing and critical facilities while staying in communication with on-site personnel via two-way radio.			
4. There are protocols to routinely check existing security measures such as fencing, locks, camera surveillance, etc. to assure they are in proper working order.			
5. There are protocols for infant security and incident response.			
6. There are measures in place to identify areas where explosive devices could be hidden.			
7. There are security protocols that address handling the media and/or VIPS.			
8. There are protocols in place that prohibit radio conversations regarding sensitive topics.			

ADVANCED PRACTICES

D. IDENTIFICATION	Yes	No	If No, Implementation Date
1. There is evidence that identification procedures for visitors, vendors and contractors are in place and include:			
a. Visitor badge/pass that identifies where visitors, vendors and contractors may travel within the facility.			
2. There is evidence that identification procedures for employees, physicians and volunteers are in place and include:			
a. ID cards that include a photo, wearer's name, department and title or credentials (i.e. MD, RN);			
b. An enforcement procedure to ensure ID is worn at all times. Exceptions are when wearing the ID would put the employee at risk for injury, in which case the ID must be carried;			
c. Procedures employees follow when the arrive at facility without their ID;			
d. Procedures for lost/stolen ID;			
e. Procedures for return of ID upon separation from employment;			
f. Restriction of access to sensitive areas defined by the facility (e.g. mother/infant, pharmacy, lab);			
g. Protocol addressing access restriction for terminated employees;			
h. Protocol requiring that resigned or terminated employees turn in equipment, access cards and keys at time of termination/resignation;			
i. Protocol identifying who is authorized to create identification and addresses the handling and storage of blank and terminated identification.			
3. There is a protocol in place to account for all employees during a crisis.			
4. There is evidence that visitors are advised that the badge/pass they receive restricts the areas they may access.			

ADVANCED PRACTICES

D. IDENTIFICATION CONT'D.	Yes	No	If No, Implementation Date
5. There is evidence that visitors are advised that their pass/badge must be visible at all times.			
6. There is evidence that outpatient identification is different from visitor ID.			
7. There is evidence that vendor badges/passes are very distinct from all others.			
8. There is evidence that contractor's badges are different from all others. They may be different for daily versus weekly contractors.			
9. There is evidence that visitor identification includes sign-in procedures.			
10. There is evidence that all vendors and/or contractors report to a central area to obtain a pass/badge and indicate where they are going.			
11. Security requires all vendors and/or contractors leave a driver's license at sign-in to be retrieved as they leave the site.			
12. There is evidence that vendors or contractors that visit on a regular basis have photo ID, the cost of which is covered by the vendor.			
13. There are protocols that address consequences for employees who fail to carry/show ID. Consequences may include:			
a. Supervisors are contacted to authorize staff that attempt to enter without ID;			
b. Staff and physicians that do not have ID must sign a log book;			
c. Staff/physicians who refuse to show ID are reported to department head and administration;			
d. After three incidents, staff member must be reported to the department head or administration; and/or,			

ADVANCED PRACTICES

D. IDENTIFICATION CONT'D.	Yes	No	If No, Implementation Date
e. After three incidents, staff are suspended.			
14. There is evidence that identification procedures for employees, physicians and volunteers include a protocol regarding handling of individuals in areas where they are not authorized.			
15. There is evidence that staff is advised that if visitors are found without a pass/badge they must be escorted to security.			

ADVANCED PRACTICES

E. SEARCHES	Yes	No	If No, Implementation Date
1. There is a protocol in place regarding:			
a. The inspection and control of security vehicles.			
b. Searches of suspicious packages and persons. Protocols should clearly define what characterizes a person/package as suspicious.			
c. Searches of employee packages or lockers.			
d. The inspection of all vehicles entering critical facilities, including cargo areas, undercarriage, glove compartments and other areas where dangerous items could be concealed.			
e. The inspection of all packages carried by visitors - including the posting of signs informing individuals that their persons/package(s) may be searched at the facilities discretion.			
2. There is a plan to implement weapons screening checkpoints at entrances.			

ADVANCED PRACTICES

F. TRAINING	Yes	No	If No, Implementation Date
1. There is documentation that indicates that all new security employees have received new employee and departmental orientation.			
2. There is evidence of pertinent annual training programs for security staff (e.g. handcuffs, use of physical force, weapons, aggressive behavior, physical security).			
3. There is evidence that security staff receive regular training, which includes:			
a. Threat assessments;			
b. National threat levels;			
c. WMD awareness as well as task specific training based on their roles in an emergency response (e.g. PPE training if they are required to wear equipments in the event of biological release or if they participate in decontamination);			
d. Specific responsibilities related to emergency management;			
e. Security policies, procedures and appropriate responses.			
4. There is evidence that the competency of security staff has been evaluated.			
5. There is evidence that security staff exercise/drill based on their role in emergency response plans (e.g. fire, bomb threats, biological threats, suspicious mail, evacuation, employee recall lists).			
6. There is evidence that security staff have tested their role in emergency response plans with local law enforcement, bomb squad, fire department, etc.			
7. There is evidence that a security orientation is provided for all new employees, volunteers, etc.			
8. There is evidence that senior security staff members mentor new security officers.			

ADVANCED PRACTICES

F. TRAINING CONT'D.	Yes	No	If No, Implementation Date
9. There is training in place for mailroom and receiving staff to identify suspicious packages.			
10. There is evidence that training includes searching of packages, patients, visitors and staff.			
11. There is evidence that security staff is trained to inspect vehicles.			
12. There is evidence that security training is developed and based on the recommendations of the International Association for Healthcare Security and Safety (IAHSS) programs.			
13. There is documented ongoing security awareness training for every employee. (Suggestion: Could be done at a departmental level.)			

ADVANCED PRACTICES

G. ACCESS	Yes	No	If No, Implementation Date
VISITORS			
1. Protocols are in place to limit or restrict the number of visitors to patients in inpatient areas. Protocol allows for case-by-case exceptions.			
2. Protocols are in place that indicate the facility, during increased threat levels, considers using only one entrance for all visitors, and ensure that visitor protocols are strictly enforced.			
3. Protocols are in place for refusal of access to people who do not have positive identification or do not have a legitimate need to enter the site.			
4. Protocols are in place to identify the owners of all vehicles at critical facilities and remove all vehicles whose owners have not been identified.			
5. There is evidence that the facility requires appropriate departments to report to a central location and escort all vendors to prevent them from wandering (i.e. pharmaceutical vendors are known to wander floor to floor and leave samples).			
6. There is evidence that security staff is notified at least 24 hrs in advance of when contractors will be working in the facility.			
a. For emergency contractor access, security is notified immediately after call is made to request contractor provide emergency assistance.			
7. There are signs posted in the emergency department indicating that the number of visitors will be limited for security or other reasons so that patients and visitors know that staff is not imposing arbitrary limitations on visitors.			
8. There are signs posted at appropriate locations of the facility noting visiting hours, access requirements, trespassing, etc.			
9. There are signs posted at points of access to instruct contractors/vendors etc. that they must coordinate their access with specific departments, i.e. media with public relations and contractors with maintenance/facilities.			

ADVANCED PRACTICES

G. ACCESS CONTINUED	Yes	No	If No, Implementation Date
VISITORS CONTINUED			
10. There is evidence that the facility evaluates if and/or when to limit use of public areas and conference facilities by outside organizations.			
11. There is evidence that the facility limits visitation and confirms that every visitor is authorized to be in a critical facility. All unidentified visitors should be escorted in critical facilities.			
DELIVERIES			
1. There are protocols regarding deliveries during and after normal working hours.			
2. There are protocols in place regarding appropriate limitation or control of access to the loading dock.			
3. There is evidence that the facility has assessed the impact of travel restrictions on deliveries.			
4. There is evidence of monitoring and securing of the loading dock area via security staff, gate, cameras, etc.			
5. There is evidence that flower deliveries must be made to one location (i.e. lobby) and require volunteers deliver.			
6. There is evidence that the facility requires food delivered from the outside be delivered to one specific location and employees must report to that location to pick up.			
7. There is evidence that the facility requires that all packages (i.e. UPS, Fed-Ex) be delivered to one central location and internal delivery made by employees.			
8. There is evidence that the facility allows only emergency deliveries after 4:30 PM, or requires after-hours deliveries go to security.			
EMPLOYEES			
1. There are protocols regarding key issuance and control.			

ADVANCED PRACTICES

G. ACCESS CONTINUED	Yes	No	If No, Implementation Date
2. Procedures are in place to terminate access to voice mail, e-mail and health information and patient accounting systems upon employee termination.			
3. There is a protocol for transporting staff in an emergency.			
4. There is evidence that staff has been educated regarding travel ban restrictions established by the state police and are aware that ID is required if traveling.			
5. The following exist, if there is a closed circuit TV system:			
a. Protocol for monitoring by security staff;			
b. Training program for staff operating/monitoring;			
c. Protocols for the use and testing of the system.			
6. There are protocols in place for use, response and testing of a panic alarm system, if in use.			
RESTRICTING ACCESS			
1. There is evidence that signs are posted at the entrance of restricted or sensitive areas indicating "Unauthorized Personnel Not Permitted" or "Authorized Personnel Only."			
2. There is evidence that the following have been evaluated for security risks: Nuclear Medicine, Interventional Radiology, Microbiology Lab, Power Plant, Water System, Pressurized Gasses, Blood Supply.			
3. There is evidence of security protocol that addresses vehicular access to emergency care areas.			
4. Protocols are in place and tested to rapidly shut down access to portions of the entire facility.			
5. Protocols are in place indicating when to limit the number of facility access points			

ADVANCED PRACTICES

G. ACCESS CONTINUED	Yes	No	If No, Implementation Date
6. Protocols identify appropriate times or events during which to reduce site ingress and egress points to an absolute minimum.			
7. There is evidence of an access control protocol for emergencies.			
8. Protocols exist to, in coordination with law enforcement, extend the facility perimeter in an emergency.			
9. Protocols exist to, in coordination with law enforcement, distance vehicle checkpoints in an emergency.			
10. Protocols are in place to ensure that employees do not prop access control points (doors/windows) open.			
11. Protocols are in place to dictate when to request assistance from local law enforcement agencies in securing the facility and access.			
12. There is evidence the facility has evaluated transportation routes and parking areas to determine whether the routes allow contact with sensitive areas. Barriers are erected to block access as appropriate to the situation.			
13. There are protocols for crowd and traffic control in an emergency.			
14. There is evidence that the facility has coordinated an emergency traffic plan with local law enforcement.			
15. There is evidence that medical gases are secured.			
16. Protocols are in place to identify locations and determine safe distances of US Postal and other delivery mailboxes.			
17. Protocols are in place to secure all emergency generators and identify areas served.			
18. Protocols are in place to identify and secure air handling units, air intake units, their location and areas served.			

ADVANCED PRACTICES

G. ACCESS CONTINUED	Yes	No	If No, Implementation Date
19. There are protocols in place to insure access integrity in the event of a power failure, if an electronic access control system is in use.			
20. There is evidence that a rapidly deployable method for blocking all vehicular traffic into and out of a facility is in place.			
21. The following exist, if metal detectors are in use:			
a. Training for staff;			
b .Protocols regarding who will be required to pass through;			
c. Protocols outlining appropriate action if alarm is activated;			
d. Protocols identifying security's response to a person's refusal to pass through metal detector;			
e. A policy identifying security's response to a person's refusal to comply with any part of policy regarding the metal detector;			
f. Policies are in place and staff is trained to respond to weapons or potential weapons brought in by patients, visitors, staff, local law enforcement and prison guards.			
22. The facility has identified when/where to erect barriers to block access to sensitive areas during increased threat levels.			
23. There is evidence that security personnel have coordinated with local law enforcement to gain an understanding of which transportation routes may be blocked during a threat level red.			
a. Determine how traffic will be controlled.			
b. Determine facility responsibility to provide support to control traffic flow.			

ADVANCED PRACTICES

G. ACCESS CONTINUED	Yes	No	If No, Implementation Date
24. There is evidence that the access control system controls access of outpatient areas into the facility.			
25. There is evidence that the facility assures terminations occur only when human resource representatives are present rather than 24/7.			
26. There is evidence that the facility requires that human resources notify security daily on a concurrent basis of all terminations or resignations so that security may restrict access accordingly.			
27. There is evidence that the facility requires that one department be responsible for terminating access to all information/phone systems as well as access to the facility.			
28. There is evidence that the facility uses a standardized form/checklist of steps to be taken for controlling terminated employee access.			
29. There is evidence that the facility assures that all personal, company and contractor vehicles at critical facility sites be secured and parked legally and at a distance from critical areas.			
30. There is evidence that the facility has evaluated and has a plan to erect more barriers to control direction of traffic flow and protect the facility by strategically positioning heavy company vehicles.			
31. There is evidence that the facility has installed collision barriers as needed, according to a hazard vulnerability analysis.			
32. There are protocols to identify when to verify that all incoming vehicles and people are authorized and that to the extent possible all vehicles, people, mail, packages, brief cases, etc., are checked entering and leaving the site and placards are placed on visiting vehicles indicating they have been checked by security.			
33. There is a plan to install/implement an access control system that provides an audit trail.			

ADVANCED PRACTICES

G. ACCESS CONTINUED	Yes	No	If No, Implementation Date
34. There is a plan to add expiration dates to access cards.			
35. There is a plan to provide security staff at each access point, if access cannot be limited.			
36. There are protocols in place to cancel or delay all non-vital facility work conducted by contractor(s) or have facility personnel continuously monitor the contractor(s) work based on threat level.			
37. The facility expedites completion of all outstanding maintenance and capital project work that could affect the security of facilities based on threat level.			

ADVANCED PRACTICES

H. CYBER SECURITY	Yes	No	If No, Implementation Date
1. There is evidence that the organization has a designated individual to coordinate the cyber security program.			
2. There are cyber security standards and guidelines that include:			
a. A data classification scheme that requires specific security measures based on the criticality of data and the risks that unauthorized access or modification would pose. The more critical the data, the more stringent security precautions should be employed.			
b. Restricting access to information that could aid terrorists.			
c. An asset classification scheme that requires specific security measures based on the risk of unauthorized access or damage to the asset or property.			
3. There is regular monitoring of these standards for compliance.			
4. There are unique user IDs and passwords and periodic password changes required.			
5. There are limited users with unrestricted or superuser privileges.			
6. There are monitored processes for removing terminated users.			
7. There is a process to modify access controls when users change jobs.			
8. There are secure measures (VPN, SSL, etc.) for employees or contractors with connectivity to the network via the Internet.			
9. There are firewalls to restrict access from the Internet.			
10. There is monitoring for unauthorized access points (modems, access points (wireless), remote control software).			
11. There are procedures for what to do when an unauthorized attempt occurs, that includes reporting, damage assessment, remediation and follow up.			

ADVANCED PRACTICES

H. CYBER SECURITY CONT'D.	Yes	No	If No, Implementation Date
12. There are hardening procedures (limit computer services and functionality to that which is needed) used by system and network administrators for critical computer systems and processes.			
13. There are security patches applied within reasonable timeframes.			
14. There is anti-virus software on network-connected systems with timely updates to virus definition files, where appropriate.			
15. There are browser settings that detect and alert users for unauthorized access to users' machines.			
16. If the organization has web-based mission critical applications, the data and the ability to process transactions is fully protected from direct access on the Web site.			
17. There are regular backups performed and off-site storage for mission critical backups.			
18. There is an information assurance program to monitor compliance with security policies.			
19. There are periodic computer vulnerability assessments performed on internal systems and for Internet connectivity as defined by HIPAA or subsequent to changes in infrastructure.			
20. There is assurance that outsourced service providers comply with the organization's security policies, standards and procedures for access to critical systems and processes. There is a signed business associates' agreement for every outsourced service provider.			
21. There are business continuity/disaster recovery plans for mission critical processes, and they are tested/updated regularly.			
22. Computer, server and telecom rooms, data closets, routers and hubs are secured.			
23. There is evidence that organizations:			
a. Conduct a cyber-security training and awareness program.			

ADVANCED PRACTICES

H. CYBER SECURITY CONT'D.	Yes	No	If No, Implementation Date
b. Participate in professional organizations and liaison with state and federal law enforcement as well as other cyber-security-related agencies to remain aware of security trends and threats.			
c. Test the strength of users' passwords.			
d. Create measures (host-based intrusion detection, access lists, etc.) to detect unauthorized activity on critical servers.			
24. There is evidence that organizations:			
a. Require strong authentication (something you have in addition to the password) where appropriate.			
b. Encrypt password files.			
c. Implement access control and/or encryption for other sensitive information based on classification.			
d. Employ data encryption when using wireless connections to networks.			
e. Monitor for unauthorized access attempts.			
f. Employ intrusion detection to detect unauthorized access from the Internet..			
g. Employ measures to detect unauthorized traffic on your network.			
h. Have a protocol for reporting any attempted cyber attacks to relevant authorities.			
i. Employ network management systems to detect failures or unauthorized connections.			
j. Require background checks and other types of screening for employees in sensitive positions.			
k. Require background checks for contractors or consultants with access to critical systems or sensitive information.			