5.4.5 When Icing conditions are suspected, use the following steps to approach a turbine:

5.4.5.1 Step 1: Stop

Stop a minimum of 1000 feet (305 m) from any turbine. In some cases, an entire string of turbines may need to be shut down to approach the turbine in question for observation.

NOTE 1: CAUTION

Do not work within 1000 feet (305 m) of an operating turbine that has ice formed on it.

5.4.5.2 Step 2: Observe from a distance

5.4.5.2.1 Observe the turbine using binoculars or similar equipment to look for signs of ice on the ground, inconsistencies on the blade, ice hanging off the nacelle and radiator area. (If ice has developed on the vehicle antenna, that is a good indicator of potential ice on the tower/blades). If it is foggy or the visibility is low, listen for ice falling.

5.4.5.2.2 Perform a remote stop. Wait 5 minutes after the machine has been shut down or once yawing has completed. Observe again with the binoculars from a safe distance (look for ice/snow that has become loose or is falling due to the nacelle's movement).

5.4.5.2.3 Yaw the turbine remotely so that the greatest Hazard above (typically ice on the blades) is on the opposite side of the tower from the entrance door. Wait 5 minutes and observe again.

5.4.5.3 Step 3: Observe closer

5.4.5.3.1 If no ice was observed, proceed to a distance of 300 feet (91 m) away and repeat the ice observation process.

5.4.5.3.2 If no ice is observed at 300 feet, one worker may approach the turbine, continually observing the turbine as they look for ice. If at any time ice is observed, the worker must return to the safe zone.

5.4.6 If the worker does not observe any Icing at the turbine, work may proceed as usual. It should be noted that ice on top of the nacelle or along the tower sections might be very difficult to see. The use of a spotter is encouraged when working near towers during Icing conditions, even if ice has not been seen.

5.4.7 Prior to exiting the turbine, personnel must verify that Icing conditions have not changed. This may occur by calling for remote observation or by checking from the top of

the turbine without stepping onto the roof of the nacelle. Consider wind speed, sun, temperature, and Precipitation that could change the characteristics related to falling. If the turbine has started shedding ice, personnel must remain in the tower until the shedding activity has stopped.

5.4.8 Turbines observed to have Icing within 1000 ft. (305m) of public roads or structures, which pose a Hazard to the road or structure, must be shutdown.

NOTE 2:

If any of these steps cannot be completed remotely, do not perform any work in the immediate area until the conditions and safe options have been properly evaluated, addressed, and re-inspected.

5.4.9 Vehicles shall not drive on turbine access roads within 300 ft. of turbines when Icing conditions are present on running turbines.

5.4.10 Vehicles shall not be parked within 300 feet of a turbine if weather conditions may cause ice buildup while the turbine is being serviced.

NOTE 3: STOP WORK

If at any time ice is observed to be shedding from the turbine, STOP WORK and do not approach the turbine.

5.5 Heavy Precipitation

5.5.1 Site management shall monitor Precipitation to provide advanced Warning of potential heavy Precipitation to employees and contractors in the field.

5.5.2 In the event of Hazardous or heavy Precipitation, site management shall issue a rain Warning to employees and contractors in the field, and an instruction to stop work.

5.5.3 All field activities shall cease, and field crews shall acknowledge the receipt of the stop work order and seek shelter in a solid structure.

5.5.4 Heavy Precipitation is often accompanied by Lightning. If employees or contractors are exiting the field due to Lightning Warnings, and are exposed to hail or heavy rain, they shall pull off the road and wait for the hail or heavy rain to stop. Severe hail may shatter windows, which could distract a driver and injure vehicle occupants.

5.5.5 When the hail or heavy rain conditions are no longer present, site management shall issue an all clear notice.

5.5.6 After a heavy Precipitation event, site management should consider road erosion and hazardous conditions.

5.6 Tornadoes

5.6.1 Site management shall monitor the weather to provide advanced Warnings of potential Tornado generating conditions to employees and contractors.

5.6.2 If a Tornado Watch is issued, then a Tornado is possible. Site management shall issue a Tornado Watch to employees and contractors in the field, and provide further instructions. At minimum, crews should prepare to seek shelter.

5.6.3 If a Tornado Warning is issued, this means that a funnel cloud has actually been spotted, or is strongly indicated on the radar. Site management shall issue an immediate instruction to move to a Tornado shelter.

5.6.4 Weather forecasting alone cannot guarantee an accurate prediction of a Tornado, and some Tornadoes do occur without a Tornado Warning. During the storm season, employees, contractors, and visitors shall use the following guidance to identify the potential for Tornado Hazards in their vicinity, and should contact site management if any of the indicators below are observed.

5.6.5 Early indicators of Tornadoes in the immediate area may include:

5.6.5.1 Strong, persistent rotation in the cloud base;

5.6.5.2 Whirling dust or debris on the ground under a cloud base – Tornadoes may not have a funnel;

5.6.5.3 Hail or heavy rain followed by either a dead calm or a fast, intense wind shift. Many Tornadoes are wrapped in heavy Precipitation, and therefore not visible;

5.6.5.4 Loud, continuous roar or rumble as this does not fade in a few seconds like thunder;

5.6.5.5 At night, small, bright, blue-green to white flashes at ground level near a thunderstorm (as opposed to silvery Lightning up in the clouds). These mean power lines are being snapped by very Strong Winds, as it may be a Tornado, and

5.6.5.6 At night, persistent lowering from the cloud base, illuminated or silhouetted by Lightning, especially if it is on the ground or there is a blue-green-white power flash underneath.

5.6.6 This procedure should be briefed to employees and contractors during tailboard meetings in storm season.

5.6.7 If personnel are instructed to seek shelter, the following actions shall be taken:

5.6.7.1 If in a building, go to interior rooms and halls on the lowest floor. Stay away from glass-enclosed places, or areas with wide-span roofs such as warehouses. Crouch down and cover your head. Corners are often safer than the middle of the wall. A bathroom, closet, office, or maintenance room with short walls are often the safest areas.

5.6.7.2 If in a vehicle, do not try to out drive a Tornado. Tornadoes can change direction quickly and can lift up a car or truck and toss it through the air. Get out of the vehicle immediately and take shelter in a nearby building. If there is no time to get indoors, get out of the car and lie in a ditch or low-lying area away from the vehicle. Be aware of the potential for flooding.

5.6.7.3 If in a turbine, employees and contractors shall descend immediately and take cover on the floor of the turbine or turbine basement, if available. Do not attempt to drive to a building.

5.6.7.4 After a Tornado Warning has passed, site management shall issue an all clear notice. Employees, contractors, and visitors will meet at the inside assembly area and perform a roll call. All employees, contractors, and visitors shall be accounted for before anyone leaves the facility.

5.7 Earthquake

5.7.1 If an earthquake occurs, personnel in the O&M building should:

5.7.1.1 Drop down to their hands and knees and seek shelter under a sturdy table or desk. If there is no shelter nearby, personnel should get down near an interior wall or next to low-lying furniture that will not fall, and protect their head and neck with their arms and hands,

5.7.1.2 Hold on to the shelter until the shaking stops,

5.7.1.3 DO NOT stand in a doorway. The doorway does not protect people from the most likely source of injury, falling or flying objects. Most earthquake-related injuries and deaths are caused by falling or flying objects (e.g., TVs, lamps, glass, bookcases), or by being knocked to the ground,

5.7.1.4 If possible, within the few seconds before shaking intensifies, quickly move away from glass, hanging objects, bookcases, china cabinets, or other large furniture that could fall. Watch for falling objects, such as bricks from fireplaces and chimneys, light fixtures, wall hangings, high shelves, and cabinets with doors that could swing open,

5.7.1.5 If available nearby, personnel should grab something to shield their head and face from falling debris and broken glass, and

5.7.1.6 If there are gas appliances on, turn them off.

5.7.2 If an earthquake occurs while personnel are outside, personnel should move away from buildings, utility wires, sinkholes, fuel, and gas lines. The greatest danger from falling debris is just outside doorways and close to outer walls. Once in the open, get down low (to avoid being knocked down by strong shaking) and stay there until the shaking stops.

5.7.3 If an earthquake occurs while driving, personnel should:

5.7.3.1 Stop as quickly and as safely as possible;

5.7.3.2 Move the vehicle to the shoulder or curb, away from utility poles, overhead wires, and out from under overpasses; and

5.7.3.3 Stay in the car and set the parking brake. Turn on the radio for emergency broadcast information. A car may jiggle violently on its springs, but it is a good place to stay until the shaking stops. If a power line falls on the car, stay inside until a trained person removes the wire.

5.7.4 If an earthquake occurs while up tower, personnel should:

5.7.4.1 Remain in the location that they are in until the shaking stops, and

5.7.4.2 Once shaking stops, monitor alerts for known aftershocks, and once it is safe, put on harness and other fall protection equipment and start to climb down tower. In the event of aftershocks, personnel should stop climbing and hold on to the ladder, and then continue climbing down. Personnel should not use lifts to climb down directly after an earthquake.

5.7.5 After an earthquake

5.7.5.1 Inspect gas services to assure there are no cracks or leaks.

5.7.5.2 If communication services are available, ensure all site personnel are safe.

5.7.5.3 Contact turbine OEM to determine if foundation inspections are necessary and ask for procedures for foundation inspections. Also, ask for an analysis of TCM or other condition monitoring alarms.

5.7.5.4 If an earthquake occurs during off-hours, site management or designated person shall arrive to site first (if conditions allow) to determine road and site conditions.

5.7.5.5 If the project owns a switchyard, contact utility for information on the condition of the transmission line where Point of Interconnect is connected before re-energizing.

5.7.5.6 Do a visual inspection of the substation and collection system before re-energizing. Also review event data from relays where trips occurred.

5.8 Cold Weather

During times of extreme cold temperatures, refer to the following chart as a guide for possible exposure limit times.

Air Temperature - Sunny Sky		**No Noticeable Wind**		**5 mph Wind**		**10 mph Wind**		**15 mph Wind**		**20 mph Wind**	
°C (approx.)	°F (approx.)	Max. work Period	No. of Breaks**	Max. Work Period	No. of Breaks	Max. Work Period	No. of Breaks	Max. Work Period	No. of Breaks	Max. Work Period	No. of Breaks
-26° to -28°	-15° to -19°	(Norm breaks) 1		(Norm breaks) 1		75 min.	2	55 min.	3	40 min.	4
-29°to -31°	-20°to -24°	(Norm breaks) 1		75 min.	2	55 min.	3	40 min.	4	30 min.	5
-32° to -34°	-25°to -29°	75 min.	2	55 min.	3	40 min.	4	30 min.	5	Non-emergency work should cease	
-35° to -37°	-30° to -34°	55 min.	3	40 min.	4	30 min.	5	Non-emergency work should cease			
-38° to -39°	-35° to -39°	40 min.	4	30 min.	5	Non-emergency work should cease					
-40° to -42°	-40°to -44°	30 min.	5	Non-emergency work should cease							
-43° & below	-45° & below	Non-emergency work should cease									

5.9 Hot Weather

5.9.1 During hot weather, refer to the following chart as a guide to recognize and prevent heat stress. The chart should only be used as a guide, and can be modified to more closely represent the climate for the site.

5.9.2 Before hot seasons start, sites shall review heat and heat stress conditions.

Heat Index Chart

Temperature (°F) vs. Relative Humidity

	10%	15%	20%	25%	30%	35%	40%	45%	50%	55%	60%	65%	70%	75%	80%
115	111	115	120	127	135	143	151								
110	105	108	112	117	123	130	137	143	151						
105	100	102	105	109	113	118	123	129	135	142	149				
100	95	97	99	101	104	107	110	115	120	126	132	136	144		
95	90	91	93	94	96	98	101	104	107	110	114	119	124	130	136
90	85	86	87	88	90	91	93	95	96	98	100	102	106	109	113
85	80	81	82	83	84	85	86	87	88	89	90	91	93	95	97
80	75	76	77	77	78	79	79	80	81	81	82	83	85	86	86
75	70	71	72	72	73	73	74	74	75	75	76	76	77	77	78

Heat Index/Heat Disorders

Heat Index	Possible heat disorders for people in higher risk groups
130 or higher	Heatstroke/sunstroke highly likely with continued exposure. Work only with site supervision approval.
105-130	Sunstroke, heat cramps or heat exhaustion likely, and heat stroke possible with prolonged exposure and/or physical activity. Recommend limiting work to 15 minutes per hour with a 45 minute break in a cool area.
90-105	Sunstroke, heat cramps and heat exhaustion possible with prolonged exposure and/or physical activity. Recommend limiting work to 30 minutes per hour with a 30 minute break in a cool area.
80-90	Fatigue possible with prolonged exposure and/or physical activity. Recommend limiting work to 45 minutes per hour with a 15 minute break in a cool place.

Source: National Weather Service

5.9.3 Heat Illness

5.9.3.1 Some risk factors for Heat Illness include:

5.9.3.1.1 High temperatures and humidity, direct sun exposure, and no breeze or wind;

5.9.3.1.2 Low liquid intake, or high caffeine drinks with little water

intake;

5.9.3.1.3 Heavy physical labor;

5.9.3.1.4 Waterproof clothing; and

5.9.3.1.5 Recent exposure to hot workplaces.

5.9.3.2 Some symptoms of Heat Exhaustion include:

5.9.3.2.1 Headaches, dizziness, or fainting;

5.9.3.2.2 Weakness and wet skin;

5.9.3.2.3 Irritability or confusion; and

5.9.3.2.4 Thirst, nausea, or vomiting.

5.9.3.3 Some symptoms of Heat Stroke include:

5.9.3.3.1 May be confused, unable to think clearly, pass out, collapse, or have seizures (fits), and

5.9.3.3.2 May stop sweating.

6. TRAINING

All Pattern employees shall be trained on this procedure on an annual basis.

7. DATA RETENTION

This procedure, appendices, and training documents are maintained on the Ops Corporate SharePoint site.

8. REVIEW

This procedure and any appendices shall be reviewed at least annually.

9. REFERENCES

9.1 SMS 502 Job Safety and Environmental Analysis Procedure

9.2 SMS 511 Working at Heights Appendix B: Wind Speed Limits

9.3 Center for Disease Control and Prevention
http://emergency.cdc.gov/disasters/earthquakes/index.asp

Pattern	SMS 504 Emergency Preparedness and Response Procedure Appendix D Hurricane Response and Recovery Plan	
Owner: **Senior Manager, EHS**	Applicability: **Pattern Operations**	
Revision No: **REV 1**	Revision Date: **7/17/2017**	Page: **1 of 5**

DOCUMENT CHANGE LOG			
DATE	**REV**	**NATURE OF CHANGE**	**AUTHOR**
1/12/2015	0	Creation of Appendix A	[redacted]
7/17/2017	1	Reviewed, no updates	[redacted]

1. OBJECTIVE

The intent of the Hurricane Response and Recovery Plan is to provide a guide for precautions and actions required if a site is the target of a severe storm/hurricane. The focus is on safe-site restoration and limited affects on environmental contamination. The guidelines effectively address how to return offsite personnel, availability of supplies, and mobilization of resources needed for restoration.

2. PREPARATION

Prior to each hurricane season, which is June 1st, all sites in areas affected by hurricanes shall ensure, that in the event, re-entry authorizations are required to enter after a hurricane, and Site Management is cleared to enter the facility.

3. RECOVERY: PHASE 1

3.1 Conduct initial site assessment (e.g. via aerial survey to view and assess the entire site using site map and aerial photos as they materialize) to inventory and document damage sustained to determine actions required for a safe return of all necessary personnel.

3.2 As soon as possible and practical, contract an environmental cleanup service vendor to coordinate the removal and proper disposal of debris and contaminated materials.

3.3 The environmental cleanup services vendor will also coordinate with the staging and storage of cleanup material that will be maintained for emergency response activities.

4. RECOVERY: PHASE 2

4.1 Site Management shall conduct an initial land-based site assessment to determine the level of site remediation.

4.2 The following areas shall be considered:

4.2.1 Debris (non-hazardous materials);

4.2.2 Blades;

4.2.3 Tower parts;

4.2.4 Nacelle parts;

4.2.5 Petroleum contamination (non-hazardous material with soil remediation);

4.2.6 Turbine oil;

4.2.7 Pad-mount transformer oil;

4.2.8 Main power transformer oil;

4.2.9 Blade pitch hydraulic oil;

4.2.10 Turbine radiators (hazardous material clean up);

4.2.11 Radiator has been ejected from top of nacelle;

4.2.12 Check if ejected radiator is leaking ethylene glycol;

4.2.13 Power lines (treat as energized state);

4.2.14 Conductors;

4.2.15 Fixtures;

4.2.16 Poles;

4.2.17 Facilities;

4.2.18 O&M building;

4.2.19 Warehouse;

4.2.20 Oil storage pad; and

4.2.21 Substation.

5. RECOVERY: PHASE 3

5.1 A two-person team will evaluate the O&M building and warehouses, substations and oil shed, and establish a command post.

5.2 A two-person (minimum) team will begin field assessment using site map, area assessment forms, camera and GPS for recording damages.

5.3 One person shall act as safety observer for those performing fieldwork activities.

5.4 Site assessments will only be conducted during daylight hours. The teams must leave the area at least one hour before nightfall.

5.5 The following materials are recommended to be obtained prior to conducting a land-based survey:

5.5.1 First aid kit;

5.5.2 Snake bite kit;

5.5.3 AED;

5.5.4 Mosquito spray;

5.5.5 Cell phone and charger/spare battery;

5.5.6 Cameras with extra storage media;

5.5.7 Sunblock;

5.5.8 Reinforced rubber boots;

5.5.9 Gloves;

5.5.10 Site map and GPS;

5.5.11 Access credentials;

5.5.12 One day supply of water, food, and toiletries;

5.5.13 Four wheel drive vehicle with full size spare tire;

5.5.14 Two 5-gallon metal gas cans and funnel;

5.5.15 Flashlights;

5.5.16 Two pairs of binoculars;

5.5.17 PPE: hard hat, safety glasses, and visibility vest; and

5.5.18 Change of clothes for extra day assessment.

5.6 The team shall perform the following actions:

5.6.1 Evaluate damage and environmental impacts;

5.6.2 Communicate damage to the OCC who shall notify other personnel within Pattern;

5.6.3 Coordinate recovery with Site Management;

5.6.4 Engineering inspections of turbine foundations and BOP equipment;

5.6.5 Contract environmental response vendor if needed;

5.6.6 Inform relevant contract counterparties, regulators, utilities and/or transmission owner/operators of recovery schedule as required;

5.6.7 Initiate insurance recovery process through Pattern's insurance department;

5.6.8 Communicate recovery plan with land owners; and

5.6.9 Notify reportable spill qualities to the applicable environmental agencies.

6. TRAINING

6.1 The Hurricane Response and Recovery Plan shall be trained on in connection with training on SMS 504 Emergency Preparedness and Response Procedure.

7. REFERENCES

7.1 SMS 504 Emergency Preparedness and Response Procedure

Pattern	RMS 448 Medium Impact BES Cyber System and Associated Cyber Asset Recovery Plan	
Owner: **Director, Information Technology**	Applicability: **Pattern Operations**	
Revision No: **REV 0**	Revision Date: **06/16/2017**	Page: **1 of 11**

DOCUMENT CHANGE LOG			
DATE	**REV**	**NATURE OF CHANGE**	**AUTHOR**
06/16/2017	0	Initial creation. Adheres to NERC CIP-009-6 Requirements.	[redacted]

1. PURPOSE

1.1 This Plan establishes the requirements and steps for Cyber Asset (CA) recovery operations and backup and restore operations with respect to BCS and their associated CAs (Electronic Access Control or Monitoring System (EACMS) and Physical Access Control Systems (PACS).

1.2 This Plan addresses applicable regulatory requirements of the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Reliability Standard CIP-009-6.

2. SCOPE

This Plan applies to all Pattern Medium Impact BCS, associated BES CAs (BCAs), and associated CAs (EACMS and PACS) as well as Pattern employees, vendors and contractors working with Pattern's Medium Impact BCS and associated CAs.

3. DEFINITIONS

BES CA (BCA): A CA that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the BES. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BCA is included in one or more BCSs.

BES Cyber System (BCS): One or more BCAs logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.

Cyber Asset (CA): Programmable electronic devices, including the hardware, software, and data in those devices.

Electronic Access Control or Monitoring System (EACMS): CAs that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BCS. This includes Intermediate Systems.

Physical Access Control System (PACS): CAs that control, alert, or log access to the PSP(s), exclusive of locally mounted hardware or devices at the PSP such as motion sensors, electronic lock control mechanisms, and badge readers.

Physical Security Perimeter (PSP): The physical border surrounding locations in which BCAs, BCS, or EACMS reside, and for which access is controlled.

4. ROLES AND RESPONSIBILITIES

4.1 CIP Senior Manager:

Responsible for leading and managing the implementation of the NERC compliance program at all NERC registered Facilities owned, operated, or managed by Pattern Operations. (Refer to RMS 417 CIP Senior Manager Assignment Procedure) In RMS 418 CIP Senior Manager Delegation Procedure, the CIP Senior Manager may delegate authority to other individual(s) where allowed by the NERC CIP Reliability Standards requirements.

4.2 CIP Senior Manager Delegate:

Responsible for performing the specific actions and assuming compliance responsibilities for delegated tasks related to NERC CIP Reliability Standards requirements. (Refer to RMS 418 CIP Senior Manager Delegation Procedure)

4.3 Director, Information Technology:

Owner of this Plan responsible for ensuring its implementation, providing the appropriate resources for implementation of the controls outlined in this Plan, and for the maintenance and update of this Plan.

4.4 System Administrator:

Responsible for performing administrative functions on the outlined CAs, and working with the Recovery Coordinator throughout this Recovery Plan process. The System Administrator is also considered a responder in the recovery plan.

4.5 Network Engineer:

Responsible for performing routine maintenance on the network and working with the Recovery Coordinator throughout this Recovery Plan process. The Network Engineer is also considered a responder in the recovery plan.

4.6 Recovery Coordinator:

The Director, Information Technology is the designated Recovery Coordinator, or recovery plan responder, tasked with leading the Recovery Plan process. In the absence of the Director, Information Technology, the System Administrator or Network Engineer may serve as the Recovery Coordinator, depending on the affected asset.

5. PLAN

5.1 Conditions for Activating the Recovery Plan (CIP-009-6, R1 Part 1.1)

5.1.1 There are numerous conditions that can take place in order to activate the Recovery Plan, for example: Hardware failure, unsuccessful software installation and/or malicious code detection.

5.1.2 Events and conditions of varied severity would activate this Recovery Plan in order to recover a Medium Impact BCS and/or an associated CA that is not functioning or not functioning properly. The severity levels are:

5.1.2.1 Low Severity (minimal to no impact to system operations): For example, one CA of a redundant pair is in need of recovery. Low severity recovery conditions may include but are not limited to:

5.1.2.1.1 A single CA is in need of recovery, and the software/hardware is readily available.

5.1.2.1.2 Multiple CAs are in need of recovery, and the software/hardware is readily available.

5.1.2.1.3 Duration to recover the CA(s) is estimated at less than 12 hours.

5.1.2.2 High Severity (Significant Impact to System Operations): For example, multiple devices including both devices of a redundant pair are in need of recovery. High severity recovery conditions may include bur are not limited to:

5.1.2.2.1 Multiple CAs are in need of recovery, and the software/hardware is not readily available.

5.1.2.2.2 Duration to recover the CA(s) is estimated at more than 24 hours.

5.2 Recovery Plan Process

5.2.1 Pre-Recovery Evaluation

5.2.1.1 When a potential need for recovery arises stemming from the failure or malfunction of a system component, the System Administrator will go through normal troubleshooting procedures. If these steps are insufficient to recover the asset, the Recovery Plan will be initiated.

5.2.2 Recovery Initiation (CIP-009-6, R1.2)

5.2.2.1 The Director, Information Technology serves as the primary Recovery Coordinator (responder). If the Director, Information Technology is not available, the applicable System Administrator or Network Engineer acts as the Recovery Coordinator and keeps the Director, Information Technology informed.

5.2.2.2 The System Administrator or other personnel who identified the need for recovery of a CA shall be the initial responder and will notify the Recovery Coordinator to initiate the Recovery Plan.

5.2.3 Recovery Plan Actions

5.2.3.1 Step 1 Assess Recovery Scope and Recovery Needs

5.2.3.1.1 The Recovery Coordinator will determine, in coordination with the System Administrator and/or Network Engineer, the affected systems and will assign a severity level to the recovery incident using the list in Section 5.1 as a guideline.

5.2.3.1.2 The Recovery Coordinator, or assignee, then notifies the impacted personnel as appropriate and for a high severity level recovery, request assistance from vendor (i.e. hardware replacement or software support) as necessary. The Recovery Coordinator should continually re-evaluate the impact of the incident throughout the process and notify affected personnel as appropriate.

5.2.3.2 Step 2 Recover the CA(s)

5.2.3.2.1 The System Administrator or Network Engineer, working with the Recovery Coordinator, will take the lead in recovering affected devices following the recovery process defined in Section 5.3 through Section 5.5 of this Plan, coordinating with vendors as necessary.

5.2.3.2.2 A detailed record of the executed restoration process is documented in the RMS 448 Medium Impact BES Cyber System and Associated CA Recovery Plan Appendix A: Checklist.

5.2.3.3 Step 3 Facilitate Lessons Learned and Follow-up

5.2.3.3.1 Upon completion of the CA restoration, the Director, Information Technology reviews the recovery plan completion

with the System Administrator, Network Engineer and/or other personnel who participated in the execution of the recovery plan.

5.2.3.3.2 The Director, Information Technology or delegate documents any lessons learned using the RMS 448 Medium Impact BES and Associated CA Recovery Plan Appendix A: Checklist. The Director, Information Technology then incorporates all needed changes to this Plan and notifies applicable personnel of the updates, as described in Section 5.8 below.

5.3. Application / Operating System Recovery

5.3.1 Pattern utilizes the following methods to perform a restoration of operating systems, applications, and files on applicable CAs (BCSs, EACMS, and PACS):

5.3.1.1 Networking Equipment: The Network Engineer performs a restore of the configuration for Cisco switches and firewalls using the backup configurations stored in Solarwinds Configuration Manager.

5.3.1.2 Windows Servers: The System Administrator performs a full system restore of Windows systems using Veeam Backup software. The backup configurations stored in the Veeam software will restore the operating system, applications, and files. In the event that only a file-level restore is required, Veeam is capable of selectively recovering individual files as needed by the recovery event.

5.3.2 IT will apply a proper recovery procedure, depending on the type of CA (Windows Server, Cisco Network Switch, Cisco Firewall etc.), for example in the event of a network device failure, the Network Engineer would retrieve the device configuration from Solarwinds Configuration manager and apply that to the network device.

5.4 Hardware Recovery

The following types of hardware form the collection of the applicable CAs (BCAs, EACMS, and PACS):

5.4.1 Networking Equipment: Pattern uses Cisco switches and Cisco Firewalls.

5.4.2 Windows Servers: Domain Controllers, Patch Management Server, Anti-Virus Server, and DMZ Jump Servers are provided by Cisco/HP

5.4.3 PACS: The system is provided by G4S Secure Integration LLC. The system includes the Network Controllers and the Network Nodes used to configure, enforce and authenticate physical access to PSPs.

5.4.4 For failed hardware components that require replacement, the following matrix should be used:

Table 1: Hardware Contact Matrix

Type of hardware	Vendor or provider	Maintenance contract #	Contact Information
Cisco Network Devices	Cisco	Via Infrastructure Internal support for Level 1 support, Infrastructure Director for escalation	Cisco TAC: 1 (800) 553-2447
Servers	Cisco		Cisco TAC: 1 (800) 553-2447X
Symmetry Connect (One Facility) PACS	G4S Secure Integration LLC	Technical Service Center Agreement, Effective Date 1st day of April, 2017 by and between G4S Secure Integration LLC	Helpdesk: 1 (844) 872-4447 (844) TSC-4G4S

5.4.5 Detailed Recovery procedures for Pattern Windows systems and network devices will be documented using an appropriate work instruction depending on the type of CA (Windows Server, Windows Workstation, Cisco Network Switch, Cisco Router etc.).

5.5 Security Requirements

This section describes the security controls to be implemented during the recovery process and to remain in place until the recovery is completed.

5.5.1 Cyber Security: Devices recovered as part of the Recovery Plan will be restored to a state that is compliant with applicable CIP-005-5 and CIP-007-6 requirements. If possible, the device will have the same security configuration as documented in the latest version of the RMS 451 Medium Impact Change and Configuration Management Process Appendix B: CA Master Security Configuration Form completed for the asset prior to the event necessitating the activation of the Recovery Plan. The RMS 451 Medium Impact Change and Configuration Management Process Change and Configuration Management Process shall be followed prior to commissioning all new CIP CAs

5.5.2 Physical Facility Security: Personnel involved in the recovery of CAs must have authorized unescorted access to CIP protected facilities, and

authorized access to confidential CIP protected information otherwise they must be escorted by authorized personnel. Escorted personnel are required to log their ingress to CIP protected areas. If an event compromises the PSP, the Recovery Coordinator must make arrangements for protecting the PSP and the affected assets, in accordance with RMS 428 Medium Impact Physical Security Plan.

5.6 Backup Process and Information Storage (CIP-009-6, R1 Part 1.3 through 1.5)

5.6.1 Pattern uses Veeam Backup software for all CAs with Microsoft Windows operating systems and Solarwinds Configuration Manager for the networking devices. The Veeam Backup server is located in the Pattern Server Room in a PSP.

5.6.2 Full Backups for all applicable CAs (i.e., workstation data, workstation images, servers, network switches, routers and firewalls) are completed on either a weekly or monthly schedule. Incremental Backups for all applicable CAs are completed on a daily basis, only capturing data that has changed since the previous Full Backup.

5.6.3 Both Full Backups and Incremental Backups of all applicable CAs are stored locally on the Veeam Backup server. Upon the completion of their weekly or monthly full backups, Pattern utilizes a backup validation tool such as MD5 or SHA1 Checksum (hashing algorithm) to validate the weekly or monthly full backups. Any identified backup failures are investigated and resolved.

5.6.4 Evidence of the backup and validation process is documented in RMS 448 Medium Impact BES Cyber System and Associated CA Recovery Plan Appendix B: Backup Validation Checklist.

5.6.5 The System Administrator and/or Network Engineer, as applicable, will preserve data, per the BCA capability, by performing a backup of the existing configuration where possible prior to recovery of the CA. If the affected CA has a corrupted drive that is related to a suspected Cyber Security Incident and a full backup of the configuration is not possible, the corrupted drive will be preserved and replaced by a new drive during the recovery process. The data preservation is used to determine the cause of Cyber Security Incidents that trigger activation of the Recovery Plan.

5.7 Recovery Plan Implementation and Testing (CIP-009-6 R2)

5.7.1 The Director, Information Technology will conduct a test of the Recovery Plan at least once every 15 calendar months. The test of the Recovery Plan may range from a paper drill, to a full operational exercise, to actual recovery of a CA.

5.7.2 The System Administrator and/or Network Engineer shall ensure that the test includes validation that a device can be recovered using its backup and

restore procedure and backup media. A sample of information used to recover the CA functionality is tested at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover CA functionality can be used to substitute the test.

5.7.3 Records to the details of the recovery test are documented in RMS 448 Medium Impact BCS Cyber System and Associated CA Recovery Plan Appendix C: Test Checklist.

5.8 Recovery Plan Review, Update and Communication (CIP-009-6 R3)

5.8.1 The Director, Information Technology shall, no later than 90 calendar days after completion of a recovery plan test or actual recovery document any lessons learned or the absence of any lessons learned using the RMS 448 Medium Impact BCS Cyber System and Associated CA Recovery Plan Appendix D: Test Follow-up and Documentation Process.

5.8.2 Changes to this Recovery Plan required as a result of testing (as documented in the lessons learned) shall be approved by the Director, Information Technology and implemented in the Plan no later than 90 calendar days after completion of a Recovery Plan test or actual recovery.

5.8.3 Changes to this Recovery Plan required as a result of changes to the roles or responsibilities, responders, or technology shall be approved by the Director, Information Technology and implemented no later than 60 calendar days after the change.

5.8.4 The Director, Information Technology will notify each person or group with a defined role in the Recovery Plan of the updates to the Recovery Plan based on any documented lessons learned or changes to the roles or responsibilities, responders, or technology.

6. TRAINING

Applicable Pattern Personnel will be trained on Pattern's Medium Impact Cyber System and Associated CA Recovery Plan. All Pattern Personnel with assigned roles and responsibilities associated with the execution of the Medium Impact Cyber System and Associated CA Recovery Plan will also receive periodic training.

7. DOCUMENTATION AND DATA RETENTION

7.1 Pattern shall retain the following documentation (including supporting information) at initial implementation; and, all records created during the execution of the process for a minimum of three (3) years or until the next scheduled NERC CIP compliance audit.

7.2 This Process will be reviewed and approved at least once every 36-calendar months after initial implementation, and will be saved as evidence on the Pattern Operations' SharePoint site:

CIP-009-6 Requirement	File Name	Comment
Requirement R1 – Recovery	RMS 448 Medium Impact BES Cyber System and Associated CA Recovery Plan	Document shall be retained.
Requirement R1 – Recovery Plan Specifications	RMS 448 Medium Impact BES Cyber System and Associated CA Recovery Plan Appendix A: Checklist	Document shall be retained.
Requirement R1 – Recovery Plan Specifications	RMS 448 Medium Impact BES Cyber System and Associated CA Recovery Plan Appendix B: Backup Validation Checklist	Document shall be retained.
Requirement R2 – Recovery Plan Implementation and Testing	RMS 448 Medium Impact BES Cyber System and Associated CA Recovery Plan Appendix C: Test Checklist	Document shall be retained.
Requirement R3 – Recovery Plan Review, Update and Communication	RMS 448 Medium Impact BES Cyber System and Associated CA Recovery Plan Appendix D: Test Follow-up and Documentation Process	Document shall be retained.

7.3 The Plan owner shall be responsible for maintaining previous approved copies of this Plan until completion of the next scheduled NERC CIP compliance audit; and, the currently approved and effective version of this process on Pattern Operations' SharePoint site.

8. REVIEW

8.1 The Director, Information Technology is responsible for reviewing this Plan as needed based upon changes to the NERC CIP Standards or changes to Pattern's approach to CA backup or recovery which impacts this Plan.

8.2 Review shall include, but is not limited to:

8.2.1 Determination that the Recovery Plan continues to meet Pattern's business needs; and

8.2.2 Confirmation the Plan continues to meet the compliance needs and requirements set forth in the applicable NERC Standard, and any applicable regional requirements.

8.3 Completion of the review shall be documented in the review log and include:

8.3.1 Date of review; and,

8.3.2 Name of person completing the review.

8.4 Any changes made to this Recovery Plan shall be documented in the Document Change Log with the:

8.4.1 Revision completion date;

8.4.2 Changes made by section identification; and,

8.4.3 Name of person completing the revision.

9. REFERENCES

9.1 NERC Reliability Standard CIP-009-6 Cyber Security: Recovery Plans for BES Cyber Systems

9.2 RMS 416 Critical Infrastructure Protection (CIP) Compliance Program

9.3 RMS 428 Medium Impact Physical Security Plan

9.4 RMS 448 Medium Impact BES Cyber System and Associated CA Recovery Plan Appendix A: Checklist

9.5 RMS 448 Medium Impact BES Cyber System and Associated CA Recovery Plan Appendix B: Backup Validation Checklist

9.6 RMS 448 Medium Impact BES Cyber System and Associated CA Recovery Plan Appendix C: Test Checklist

9.8 RMS 448 Medium Impact BES Cyber Systems and Associated CA Recovery Plan Appendix D: Test Follow-up and Documentation Process

9.9 RMS 451 Medium Impact Change and Configuration Management Process

9.10 RMS 451 Medium Impact Change and Configuration Management Process Appendix B: CA Master Security Configuration Form

Pattern	RMS 428 Medium Impact Physical Security Plan	
Owner: **Manager, Operations Control Center**	Applicability: **Pattern Operations**	
Revision No: **REV 1**	Revision Date: **09/17/2018**	Page: **1 of 21**

Management Approval:

By: _____
Signature

Name: Lance Haacke
Printed Name

Title: Manager, OCC

DOCUMENT CHANGE LOG			
DATE	REV	NATURE OF CHANGE	AUTHOR
06/22/2017	0	Initial Draft of Procedure	[redacted]
04/30/2018	1	Removed reference to fire codes	[redacted]
9/17/2018	1	Completed annual review with no changes required.	[redacted]

Pattern

RMS 428 Medium Impact Physical Security Plan

1. PURPOSE

1.1 To establish how physical access to Medium Impact Bulk Electric System Cyber Systems (BCS) and associated Cyber Assets (CA) are protected to minimize security incidents that could impact the safety of personnel, and reduce any BES reliability risk.

1.2 The Plan addresses applicable regulatory requirements found in the North America Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Security Standard CIP-006-6 (referred to hereafter simply as CIP-006). The objective of the Plan is to indicate how the physical security controls for Medium Impact BCS and associated CA(s) in use at Pattern's facilities are configured and documented.

1.3 The physical security of Low Impact facilities is covered in RMS 430 Low Impact Physical Security Control Plan.

2. SCOPE

This Plan is applicable to all Medium Impact BCS and associated CA(s) in use at all of Pattern's facilities.

3. DEFINITIONS

BES Cyber Asset (BCA): A CA, that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected facilities, systems, and equipment shall not be considered when determining adverse impact. Each BCA is included in one or more BCSs.

BES Cyber System (BCS): One or more BCA(s) logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.

Cyber Assets (CA): Programmable electronic devices including the hardware, software, and data in those devices.

Electronic Access Control or Monitoring Systems (EACMS): CA(s) that perform electronic access control or electronic access monitoring of the ESP(s) or BCS. This includes Intermediate systems.

Electronic Security Perimeter (ESP): The logical border surrounding a network to which BCS(s) are connected using a routable protocol.

External Routable Connectivity (ERC): The ability to access a BCS from a CA that is outside of its associated ESP via a bi-directional routable protocol connection.

Individual with Authorized Unescorted Physical Access: An individual with a valid and acceptable Personnel Risk Assessment (PRA) on file with Human Resources, has completed the mandatory CIP training, and has been granted full access within the PSP by the Manager, OCC.

Interactive Remote Access: User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a CA that is not an Intermediate System and not located within any of the Responsible Entity's ESP(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) CA used or owned by the Responsible Entity, 2) CA used or owned by employees, and 3) CA used or owned by vendors, contractors, or consultants. Interactive Remote Access does not include system-to-system process communications.

Intermediate System: A CA or collection of CAs performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the ESP.

Local Access Control and Monitoring (LACM): When local Pattern personnel or hired security personnel take responsibility for controlling, monitoring and logging access to the PSP Physical Access Point.

Operations Control Center (OCC): The PSP located in Pattern's Houston office where personnel work, monitor, and control the facilities owned and/or operated by Pattern on a real-time basis, 24-hours per day/7-days per week.

Physical Access Control System Microcontroller – (PACS) Microcontroller: Electronic device that facilitates access, monitoring and logging of physical access and resolves input information with the central PACS Server.

PACS Device: PACS Microcontroller or PACS Server.

Physical Access Control List (PACL): A list containing the names of individuals with unescorted physical access to PSP.

Physical Access Point: A point of ingress or egress to a PSP which is subject to access control requirements.

Protected Cyber Assets (PCA): One or more CAs connected using a routable protocol within or on an ESP that is not part of the highest impact BCS within the same ESP. The impact rating of PCAs is equal to the highest rated BCS in the same ESP.

PSP Monitor: An individual designated by Pattern to take over the LACM for the PSP in the event that the PACS Devices fail.

Physical Security Perimeter (PSP): The physical border surrounding BCS components. The OCC and the Server Room are Pattern's two PSPs.

OCC Server Cage (Server Room): The PSP located in Pattern's Houston office that contains BCS components.

4. ROLES AND RESPONSIBILITIES

4.1 CIP Senior Manager:

Responsible for leading and managing the implementation of the NERC compliance program at all NERC registered facilities owned, operated, or managed by Pattern Operations. (Refer to RMS 417 CIP Senior Manager Assignment Procedure.) In RMS 418 CIP Senior Manager Delegation Procedure, the CIP Senior Manager may delegate authority to other individual(s), where allowed by the NERC CIP Reliability Standards requirements.

4.2 CIP Senior Manager Delegate:

Responsible for performing the specific actions, and assuming compliance responsibilities for the assigned NERC CIP Reliability Standards requirements. (Refer to RMS 418 CIP Senior Manager Delegation Procedure.)

4.3 Manager, OCC:

Responsible for the operational activities performed by personnel at the OCC. Responsible for approving OCC personnel cardholders into the PACS database as well as performing a quarterly reviews of OCC cardholders in the PACS database to ensure users who have access are authorized accordingly

4.5 OCC Operator:

Responsible for ensuring all requirements of this procedure are met for all visitors to the OCC.

4.6 Individual with Authorized Unescorted Physical Access:

Responsible for adhering to the security control measures of this procedure and for escorting and logging in individuals without authorized Unescorted Access into any PSP.

4.7 Director, Information Technology:

Responsible for approving the Server Room cardholders into the PACS database, as well as performing a quarterly review of the Server Room cardholders in the PACS database to ensure users who have access are authorized accordingly.

4.8 HR Assistant:

Responsible for communicating new hires and access based upon company needs and policies.

4.9 Corporate Facilities Manager:

Responsible for physically programming PSP access cards and maintaining the PACS database. Also responsible for managing service agreements with third-party security monitoring organizations.

4.10 Senior Manager, Regulatory Compliance:

Responsible for creating, maintaining, and distributing the RMS 437 Medium Impact Cyber Security Policy Appendix A: CIP Exceptional Circumstances Procedure. The Senior Manager, Regulatory Compliance is also responsible for reviewing Appendix A: CIP Exceptional Circumstances Procedure on an annual basis, but at least every 15 calendar months prior to the CIP Senior Manager approving the policy.

5. PHYSICAL SECURITY PLAN

5.1 Physical Security Perimeter (PSP) Specifications (CIP-006-6, Requirement R1, Parts 1.1, 1.2, 1.4 and 1.10.)

5.1.1 BCS and associated BCA within PSP:

Pattern identifies the CA(s) within an ESP, as well as, CA(s) used in EACMS for the ESP. After the CA(s) are identified, Pattern conducts an assessment of the physical location for all systems. During the physical assessment, the PSP and infrastructure protecting those systems are also identified. Pattern utilizes the following guidelines when constructing and/or hardening the PSP protecting identified cyber systems and associated assets:

5.1.1.1 Development of the following physical security defense-in-depth requirements for locations containing Medium Impact BCS and their associated CA(s) to include:

5.1.1.1.1 Two-factor authentication access is used consisting of access card and biometric readers.

5.1.1.1.2 Any offices adjacent to a PSP having uncontrolled external access and a Physical Access Point, have controlled access installed at the Physical Access Point between the office and the PSP.

5.1.1.1.3 A separate PACS has been installed to manage and alert the OCC to meet the 15-minute requirement in CIP-006.

5.1.1.1.4 Solid wood or metal doors have been installed.

5.1.1.1.5 All entry doors provide free egress when exiting either PSP locations.

Ingress card and biometric readers are installed to help with monitoring and logging of access into both PSP locations (OCC Room & OCC Server Cage in the Server Room).5.1.1.2 Cabling and other non-programmable communication components are used for connecting CA(s) within the same ESP. CA(s) located outside of the PSP are protected by one of the following methods:

5.1.1.1.6 Cabling and components are protected with conduit or closed cable trays;

5.1.1.1.7 Data is encrypted;

5.1.1.1.8 Status of communication links are monitored, and alarms or alerts for communication failures are sent to those individuals listed in the RMS 447 Medium Impact Cyber Security Incident Response Plan (MI-CSIRP) within 15 minutes of detection; or,

5.1.1.1.9 Other equally effective logical protection will be used and noted in site specific documents.

5.1.1.3 Pattern uses a completely enclosed PSP to protect applicable CA(s) wherever possible. When a completely enclosed physical border cannot be established, an alternative measure to control physical access will be deployed and documented.

5.1.2 Identification and Measures to Control Entry at PSP(s) Physical Access Point(s).

5.1.2.1 During the physical assessment process described in Section 5.1.1 above, PSP Physical Access Point(s) have been identified. All access points installed provide free egress to exit either PSP. Physical Access Point(s) that allow ingress have an access control card and biometric reader to gain entry, and include alarm contacts to monitor door status.

5.1.2.2 Identification of all PSP Physical Access Point(s) and measures to control entry and the electronic measures to control entry are documented in the PACL.

5.1.2.3 Pattern validates security measures at Physical Access Point(s) with programming in the PACS during the Maintenance and Testing process as per the RMS 432 PACS Maintenance and Testing Program. Testing to validate the PACS are performed initially at installation; and then the Maintenance and Testing will be performed at least once every 24 calendar months.

5.1.3 Processes, Tools and Procedures to Monitor Physical Access to PSP

5.1.3.1 The Physical Access Point(s) at either PSP have card access for monitoring and reporting in the PACS, and alarm points for OCC notification. Egress only Physical Access Point(s) will have alarm points.

5.1.3.2 Alarm points are monitored by a third party security monitoring organization named G4S. Upon receipt of an alarm, G4S will notify the OCC within 15 minutes of detection, and OCC staff will immediately investigate the alarm. The OCC will notify all affected parties (Manager, OCC; Director, IT; etc.) and document the incident in accordance with this procedure, along with RMS 447 Medium Impact Cyber Security Incident Response Plan (MICSIRP).

5.2 Physical Access Controls (CIP-006-6, Requirement R1, Parts 1.1 & 1.2)

5.2.1 Appropriate Use of Physical Access Controls

5.2.1.1 The appropriate use of Physical Access Controls is the responsibility of Pattern employees and non-employees (Contractors, service vendors, etc.) who have authorized unescorted physical access into a PSP. Pattern trains and conducts periodic security awareness campaigns for all individuals with unescorted physical access into a PSP.

5.2.1.2 RMS 435 Medium Impact Cyber Security Training and Security Awareness Program document covers the appropriate and inappropriate use of Physical Access Controls, including but not limited to:

5.2.1.2.1 Tailgating through a Physical Access Point,

5.2.1.2.2 Sharing access cards,

5.2.1.2.3 Disabling an alarm contact, or

5.2.1.2.4 Intentionally circumventing a Physical Access Point.

5.2.1.3 Pattern prohibits the inappropriate use of Physical Access Controls. The inappropriate use of Physical Access Controls may result in disciplinary action, up to and including revocation of authorized unescorted physical access, and/or termination.

5.2.1.4 Examples of proper use of Physical Access Controls include, but are not limited to:

5.2.1.4.1 Access Control Identification Card:

5.2.1.4.1.1 Used for identification purposes.

5.2.1.4.1.2 Used for access to Pattern's facilities.

5.2.1.4.1.3 Is displayed at the waist or higher when the individual is on duty.

5.2.1.4.1.4 Issued to a specific individual and is not transferable or shared.

5.2.1.4.1.5 Will be deactivated immediately by the Corporate Facilities Manager as directed by the Manager, OCC or Director, Information Technology after the card holder has reported it lost or stolen or the Manager, OCC or Director , Information Technology deems necessary.

5.2.1.4.1.6 Must be returned immediately to the Manager, OCC or Director, Information Technology when access is no longer needed (i.e., job change, retirement, resignation, termination, etc.), or at the request of Pattern management or Human Resources.

5.2.1.4.2 Access Control Identification Card Reader Entry Door:

5.2.1.4.2.1 Displays green when access is granted.

5.2.1.4.2.2 Displays red when access is unauthorized or access card is not recognized.

5.2.1.4.2.3 Will alarm if it is tampered with or removed.

5.2.1.4.2.4 For normal operations, an individual's issued access card will be used for the associated card reader.

5.2.1.4.2.5 Will be closed properly and verified closed by the individual prior to entering and after exiting. If the door does not close properly, the problem will be reported immediately to the OCC for resolution.

5.2.1.4.2.6 It is considered improper use of a door when an Individual with Authorized Unescorted Physical Access allows another individual entry through the door by swiping their issued card. This is referred to as piggybacking or tailgating and is

prohibited. (Note: The only exception is when an Individual with Authorized Unescorted Physical Access is escorting a visitor or visitors).

5.2.1.4.2.7 An individual will not loiter with access point doors held open.

5.3 LACM of Access Point(s) (CIP-006-6, Requirement R1, Parts 1.1, 1.2 & 1.9)

Normally, access to Pattern's PSPs will be handled electronically using PACS microcontrollers. If manual entry is required due to failure of a PACS Microcontroller, maintenance on a card reader, etc., access to the PSP will be controlled manually. When the PACS Device is inoperable and unable to control access and/or monitor the identified PSP Physical Access Point(s), the OCC will receive an alarm notification within 15 minutes of the detection and will initiate the following:

5.3.1 LACM Process

When the OCC has an operational need to locally control access and monitor a PSP physical control point or PACS Device, the OCC will first contact the Manager, OCC or Director of Information Technology for approval. The OCC will then implement the LACM process for the PSP Physical Access Point, except during an emergency or CIP Exceptional Circumstance (reference RMS 437 Medium Impact Cyber Security Policy).

5.3.1.1 Requirement to Begin Process: When a PACS Device is found to be inoperable by an Individual with Authorized Unescorted Physical Access to the PSP; the OCC will be notified at the phone number posted at the PSP Physical Access Point. The OCC will also be notified by alarm if the PACS is disabled. The OCC will initiate the LACM process.

5.3.1.2 Approval: Manager, OCC or Director of Information Technology's approval is needed.

5.3.1.3 Definition of PSP Monitor: The individual assigned to locally monitor and control a PSP Physical Access Point. If the PSP Monitor does not have authorized unescorted physical access to the PSP, the Manager, OCC or Director of Information Technology is responsible for explaining to the PSP Monitor the responsibilities for monitoring and controlling the PSP Physical Access Point with instructions prohibiting their physical entry to the PSP. The PSP Monitor will not enter the PSP, except during an emergency or CIP Exceptional Circumstance, (reference RMS 437 Medium Impact Cyber Security Policy Appendix A: CIP Exceptional Circumstances Procedure).

5.3.1.4 Access Control List to Verify Access: The Corporate Facilities Manager will provide the PSP Monitor the most recent access control list for the PSP Physical Access Point(s). The list will be used by the PSP

Monitor to verify individuals with authorized unescorted physical access to PSP.

5.3.1.5 LACM Documented Records: When the LACM process is initiated, the following will be documented by the OCC and communicated to the Manager, OCC and/or Director, Information Technology and any individual at the designated PSP Physical Access Point:

5.3.1.5.1 Specific LACM location,

5.3.1.5.2 Reason for the LACM,

5.3.1.5.3 Name of Approver,

5.3.1.5.4 Name and unique ID number, if available, of PSP Monitor,

5.3.1.5.5 LACM start date and time, and

5.3.1.5.6 LACM target end date and time.

5.3.1.5.7 The OCC is responsible for coordinating the LACM process and notifying the Manager, OCC and/or Director, Information Technology when the operation of the PACS microprocessor device at the PSP Physical Access Point has been restored.

5.3.1.6 Log Access: The PSP Monitor will log access in the manual log found in OMS 230 Visitor Access for all individual(s) requiring entry and with authorized unescorted physical access according to the access list for the PSP Physical Access Point(s).

5.3.1.7 Monitor and Report Suspicious Activity: The PSP Monitor will report any suspicious activity immediately to the OCC. Suspicious activities may include, but are not limited to: (1) individual(s) showing unusual interest by loitering, photographing or video recording at the PSP; (2) strong odors around or coming from the PSP; and/or (3) unusual noises/sounds coming from inside the PSP. If the PSP Monitor determines the PSP is unsafe, they should leave and call 911 as soon as possible. The PSP Monitor will be instructed to document as many details about the situation as possible and report them to the OCC.

5.3.1.8 Conclude Manual Access/Monitoring Process: When operation of the PACS microprocessor has been restored and the OCC resumes monitoring of the PSP, the PSP Monitor, Manager, OCC and/or Director, Information Technology will be notified of conclusion of LACM process at PSP Physical Access Point(s) being manually monitored.

5.3.2 Visual Observation of PSP Physical Access Point(s)

The PSP Monitor will observe visually the PSP Physical Access Point(s) during the LACM process. The PSP Monitor will monitor and control physical access, which may involve more than one PSP Physical Access Point. The PSP Physical Access Point(s) will be located within the visual line of sight, or an additional PSP Monitor will be used. The visual line of sight does not include monitoring via a video management system or CCTV system.

5.4 Review of Access Authorization Requests and Revocation of Access Authorization (CIP-006-6, Requirement R1, Parts 1.1 & 1.2)

Pattern's Manager, OCC and Director, Information Technology are responsible for authorizing who has authorized unescorted physical access to any PSP in the PACS. The Corporate Facilities Manager, at the direction of the Manager, OCC and Director, Information Technology, will grant or remove an individual's access in the PACS, as well as run reports to allow them to verify only authorized individuals continue to have unescorted physical access. Authorized unescorted physical access will only be granted to those individuals who have a business need, have completed the required CIP training, and a valid Personnel Risk Assessment (PRA) is on file with Human Resources. In the event of an emergency or CIP Exceptional Circumstance, access to the PSP may be granted or removed by the Manager, OCC and Director, Information Technology. All physical access authorization requests and revocations will be executed and configured in the PACS by the Corporate Facilities Manager at the direction of the Manager, OCC and Director, Information Technology.

5.5 Physical Access Controls (CIP-006-6, Requirement R1, Parts 1.1 & 1.2)

The following methods for controlling access to PSPs and/or PACS will be used:

5.5.1 Physical Access Controls

The PSP Physical Access Point(s) are protected by the following system of PACS devices:

5.3.1.9 Badge System Controller (BSC):

This physical access control system microcontroller works in tandem with POPHOUKMS01 to control physical access by locking\unlocking doors to PSP areas based on permissions appointed to badge and fingerprints. Based on an AMAG M2150 2DBC system, the BSC manipulates voltage to activate or release the lock systems on doors in the OCC Room and the OCC Server Cage. Built-in battery attached allows the BSC to hold the locks for an hour or so in the event of complete power failure

5.3.1.9.1 POPHOUKMS01:

Windows Server 2012 R2 virtual machine hosts Biostar server software, which manages the configuration, access permissions and monitoring of user access card and thumbprint. It also hosts Symmetry Professional application used for configuration of the Badge System Controller (BSC). POPHOUKMS01 provides role of Physical Access Control System Server and communicates with badge readers and BSC over ESP-protected ethernet

5.3.1.9.2 Badge Reader OCC Room (INF):

Tamper-resistant fingerprint and badge reader presents dual-factor authentication for users entering OCC Server cage in the server room. Communicates with POPHOUKMS01 over ESP-protected ethernet.

5.3.1.9.3 Badge Reader OCC (NOC):

Tamper-resistant fingerprint and badge reader presents dual-factor authentication for users entering OCC room. Communicates with POPHOUKMS01 over ESP-protected ethernet.

G4S monitors and controls all PSP Physical Access Point(s), 24-hours per day/7-days per week, through the use of the PACS Devices. Activity at all PSP Physical Access Point(s) are recorded and stored through Badge System Controller and Biostar software on POPHOUKMS01.

5.5.2 Card Key and Fingerprint

The Corporate Facilities Manager will manage activation and deactivation of access cards for unescorted physical access to PSP via the PACS Device. Each person with authorized unescorted physical access to a PSP will be issued an access card by the Corporate Facilities Manager that includes the following information:

5.5.2.1 Individual's Name;

5.5.2.2 Department; and

5.5.2.3 Photograph.

In addition, the user's fingerprint will also be enrolled and associated with his access profile to be used as a second authentication factor in combination with the access card.

5.5.3 Security Personnel

In the event the PACS is unavailable, a PSP Monitor will be deployed according to the LACM process described in Section 2.3.1.

5.6 Monitoring Physical Access (CIP-006-6, Requirement R1, Parts 1.4, 1.5 & 1.6)

The following methods are used to monitor physical access to PSP and/or PACS:

5.6.1 Monitoring Physical Access

G4S monitors physical access to PSPs and/or PACS Devices 24-hours per day/7-days per week, using PACS. PACS will send alarms to G4S for immediate response and resolution. G4S will notify the OCC within 15 minutes of detecting an alarm for entry in which there was no prior notification or detection of unauthorized access attempts, etc. The OCC will follow the alarm resolution steps and reporting as outlined in section 5.1.3 of this document, along with RMS 447 Medium Impact Cyber Security Incident Response Plan (MICSIRP). The OCC documents any notifications for alarms in the PACS which are reviewed using a two-person integrity check/review by the Manager, OCC.

5.6.2 Alarm Systems

Pattern uses an alarm system at each PSP Physical Access Point and PACS Device, which sends an alarm for a forced or held open door, key override, use of invalid or unknown card, tampering with card reader, PACS Microcontroller power failure, and communication failure of card reader or PACS Microcontroller. A third party is responsible for monitoring all alarm points at PSPs and PACS Devices 24-hours per day/7-days per week. The third party will notify the OCC of any alarms within 15 minutes of detection. The OCC is responsible for documenting each alarm from the PACS.

5.6.3 Human Observation of PSP Access Points

5.6.3.1 During periods when the PACS is unavailable for monitoring, the Manager, OCC will coordinate and arrange for the deployment of security personnel to be PSP Monitors according to the LACM process described in Section 2.3.1. The PSP Monitor(s) will be responsible for monitoring the PSPs and/or PACS Devices to ensure no unauthorized physical access. Suspicious activity at the PSP will be reported by the PSP Monitor(s) immediately to the OCC.

5.6.3.2 If the PSP Monitor(s) does not have authorized unescorted physical access, they will be instructed not to enter the PSP and will control entry to the PSP from outside. The only exception for entry is during an emergency or CIP Exceptional Circumstance, (reference RMS 437 Medium Impact Cyber Security Policy Appendix A: CIP Exceptional Circumstances Procedure).

5.7 Logging Physical Access (CIP-006-6, Requirement R1, Parts 1.8 & 1.9)

The following methods will be used for logging physical access to the PSPs and PACS:

5.7.1 Logging Physical Access

Pattern has installed a computerized PACS for logging access at each PSP Physical Access Point. A NERC CIP PSP Visitor Log is also maintained at each PSP Physical Access Point. The NERC CIP PSP Visitor Log is currently a manual log. The logging method uniquely identifies the individual by name, date and time of physical entry to the PSP 24-hours per day/7-days per week. The date and time of access is defined as the time in which the Individual with Authorized Unescorted Physical Access enters the PSP. Refer to OMS 230 Visitor Access for specific procedures related to the NERC CIP PSP Visitor Log.

5.7.2 Computerized Logging

Computerized logging system for PSP Physical Access Control is provided through the combined functions of the PACS microcontroller (Badge System Controller) and the PACS server (POPHOUKMS01)

5.7.3 Manual Logging

Manual logging is maintained and controlled by the OCC. The NERC CIP PSP Visitor Log is used by the OCC to log access if the PACS is unavailable. Visitors with authorized unescorted physical access to the PSP must complete the Visitor Access Log. Visitors to the OCC and PSP Server Room must follow OMS 230 Visitor Access Procedure.

5.7.4 Access Log Retention

All access logs (electronic or manual) are retained for a minimum of 90 days. Logs related to reportable incidents will be kept in accordance with Section 7.0 'Document and Data Retention'. The OCC retains the electronic access control logs generated by PACS. Paper or manually recorded NERC CIP PSP Visitor Logs are also retained by the OCC.

5.8 Physical Security System Changes and PSP Walk-Downs (CIP-006-6, Requirement R1, Parts 1.1, 1.2 & 1.10)

If the physical security controls for a PSP and/or PACS is required, for example, adding an additional physical entry point to a PSP, or changing an access door to a PSP, or installing a new PACS, etc., Pattern will follow the appropriate change process below:

5.8.1 Physical Security System Changes

5.8.1.1 Notify the Manager, OCC and/or Director, Information Technology at least 30 days in advance, of any plan to change a physical

security system, or plans for a physical security system redesign or reconfiguration, including, but not limited to:

5.8.1.1.1 Adding or removing Physical Access Point(s) to the PSP;

5.8.1.1.2 Creating or modifying penetration points within the PSP (i.e., adding an air conditioning/ventilation duct, expanding a cable tray that penetrates one or more walls);

5.8.1.1.3 Adding, modifying or removing Physical Access Controls (i.e., doors, card readers, key cores, microcontrollers);

5.8.1.1.4 Adding, modifying or removing monitoring controls (i.e., alarm contacts, video cameras);

5.8.1.1.5 Adding, modifying or removing logging controls (i.e. PACS Devices); or,

5.8.1.1.6 Adding, modifying, or removing a PSP.

5.8.1.3 Upon notification, the Manager, OCC and/or Director, Information Technology will review the planned change and initiate a change ticket. The OCC and/or Information Technology team will work with Pattern Management on the viability of the proposed plan for change. After the OCC and/or Information Technology team and Pattern Management complete the review and the planned change is approved, the Manager, OCC and/or Director, Information Technology will determine if the change requires vendor support and will start the internal purchasing process for the purchase and installation. A change management ticket will be created to track the planned change. Pattern will update the site specific PACL. The Manager, OCC and/or Director, Information Technology will combine the new site specific PACL and store the physical security records on Pattern Operations' SharePoint site.

5.8.2 Physical Security Review of PSP

Pattern has implemented the following review process for a PSP and the associated Physical Access Controls when there is a proposed addition, deletion or modification. The Corporate Facilities Manager is required to contact the Manager, OCC and/or Director, Information Technology at least 30 days prior to the proposed implementation of a new PSP or for any modifications to an existing PSP.

5.8.2.1 Prior to Review

Prior to scheduling a physical security review for a PSP with Pattern Management, the Manager, OCC and/or Director, Information Technology will:

5.8.2.1.1 Review prior site security assessment(s), as applicable;

5.8.2.1.2 Review PACL for the site;

5.8.2.1.3 Review the Physical Access Controls, alarms and alarm instructions from the PACS for verification during the walk-down;

5.8.2.1.4 Verify and update alarm instructions and call-outs in the PACS, as applicable; and,

5.8.2.1.5 Schedule the physical security walk-down with an OCC or IT representative.

5.8.2.2 Physical Security Walk-down

A representative from the OCC and/or Information Technology team will perform the following activities, where applicable, during a PSP physical security walk-down:

5.8.2.2.1 Verify the PACS at the PSP Physical Access Point meets identified specifications and controls unauthorized access attempts;

5.8.2.2.2 Verify the existence of any alternative penetration points (i.e., air ducts, windows, cabling or other non-programmable communication components, etc.);

5.8.2.2.3 Verify NERC CIP PSP Visitor Log is located at the PSP Physical Access Point; and,

5.8.2.2.4 Ensure alarm(s) at access point(s) are tested.

5.8.2.3 Action Plan Documentation

After completion of the walk-down the Manager, OCC and Director, Information Technology will develop an action plan. The action plan will be provided to the OCC first if any issues are identified during the physical security walk-down that need immediate remediation. The OCC will contact the Manager, OCC and/or Director, Information Technology after completing the remediation tasks in the action plan. The implementation of any changes will be documented by a change ticket. The Manager, OCC and Director, Information Technology will update the

PACL. The physical security records for the site will be combined, updated and stored in Pattern Operations' SharePoint site.

5.9 OCC Incident Response Process (CIP-006-6, Requirement R1, Parts 1.5 & 1.7)

5.9.1 Incident Response

5.9.1.1 Pattern has developed a Cyber System Incident Response Plan (CSIRP) and identified a CSIRP Team with defined roles and responsibilities for a cyber related security event or incident, (see RMS 447 Medium Impact Cyber Security Incident Response Plan). The OCC will comply with the CSIRP and will report to the CSIRP Team in accordance with the plan.

5.9.1.2 The OCC will follow the CSIRP for reporting security events or incidents at Pattern. At the time of a suspected security event or incident, PSP unauthorized physical access or an alarm notification from a PACS Device occurs and is identified by G4S and notification is made to the OCC. The following information will be documented, if known:

5.9.1.2.1 Date, time and location of facility;

5.9.1.2.2 Brief description of the incident;

5.9.1.2.3 Identify all Individuals involved;

5.9.1.2.4 What assets or system(s) were impacted?

5.9.1.2.5 Was it an actual or suspected physical attack?

5.9.1.2.6 Were any security devices or system rendered inoperable?

5.9.1.2.7 Was there an unauthorized access to the PSP?

5.9.1.2.8 Name and contact information for the OCC individual collecting the information, and a designated point of contact; and

5.9.1.2.9 The supervisor's name and contact information for the person reporting the incident to the OCC.

5.9.1.3 The OCC will make every attempt to gather as much information as possible at the time the incident is reported.

5.9.2 Unauthorized Access to PSP, or Suspected Physical Security Incidents.

5.9.2.1 The OCC will immediately contact the Manager, OCC for suspected unauthorized access to a PSP, or for suspected physical

security incidents. The OCC will provide the information collected about the incident (refer to Section 2.9.1 above).

5.9.2.2 The OCC will then start an investigative draft report for the suspected physical security incident. A copy of the draft report will be forwarded to the Manager, OCC. The Manager, OCC is responsible for suspected unauthorized access to a PSP or suspected physical security incidents.

6. VISITOR CONTROL PROGRAM

6.1 Visitor Control Program (CIP-006-6, Requirement R2, Parts 2.1, 2.2 & 2.3)

6.2 The PSP Visitor Control Program is detailed in OMS 230 Visitor Access.

7. PACS MAINTENANCE AND TESTING PROGRAM

7.1 PACS Maintenance and Testing Program (CIP-006-6, Requirement R3, Part 3.1)

7.2 The PACS Maintenance and Testing Program is described in RMS 432 PACS Maintenance and Testing Program.

8. DOCUMENTATION

The PACL contains the names of individuals with authorized unescorted physical access to a PSP. The list is maintained by the Manager, OCC and Director, Information Technology. The Manager, OCC and Director, Information Technology are responsible for adding, deleting, periodically reviewing and updating the PACL for their assigned PSPs.

9. REVIEW

9.1 This plan shall be reviewed as needed, annually, or no longer than once every 15 calendar months.

9.2 The CIP Senior Manager is responsible for the oversight of this plan.

9.3 The review of this plan shall include, but is not limited to:

9.3.1 Determines that this plan continues to meet the business needs of Pattern Operations.

9.3.2 Confirms that this plan meets the applicable NERC CIP Reliability Standards requirements.

9.4 Completion of the review shall be documented in the review log indicating:

9.4.1 Date of review; and

9.4.2 Name of person completing the review.

9.5 Any changes made to this Plan shall be documented in the Document Change Log within this document indicating:

9.5.1 Revision completion date;

9.5.2 Changes made and to what sections; and

9.5.3 Name of person completing the revision.

10. DOCUMENTATION AND DATA RETENTION

10.1 The CIP Senior Manager shall retain the following documentation, and any supporting information produced from the execution of this Plan when it is initially implemented, and for each review thereafter, as evidence on the appropriate Pattern Operations' SharePoint site:

CIP-006 Requirement	File Name	Comment
R1 – Physical Security Plan	RMS 428 Medium Impact Physical Security Plan	Document will be retained, as well as any completed supporting information.
R3 – PACS Maintenance and Testing Program	RMS 432 Physical Access Control System Maintenance and Testing Program	Document will be retained, as well as any completed supporting information.

Supporting information:

Item	File Name	Comment
PSP Diagrams	CIP-006-6 <site name>_PSP_<version#> .vsdx	Diagram(s) documenting Physical Access Controls and PSP Physical Access Point(s).
Visitor Access Control Program	OMS 230 Visitor Access.docx	Document outlines the OCC Visitor Access Control Program.

10.2 The CIP Senior Manager shall be responsible for maintaining current and previously approved copies of the Physical Security Plan on Pattern Operations' SharePoint site.

10.3 At a minimum, the OCC shall retain all compliance data, procedures, documents, studies, and any associated evidentiary records during the time period between regional NERC CIP audit cycles.

11. TRAINING

Training on this Plan will be given by the procedure owner to the CIP stakeholders on an as needed basis.

12. REFERENCES

12.1 NERC Reliability Standard CIP-002-5.1 Cyber Security - BCS Categorization

12.2 NERC Reliability Standard CIP 006-6 Cyber Security – Physical Security of BCSs

12.3 OMS 230 Visitor Access

12.4 RMS 437 Medium Impact Cyber Security Policy

12.5 RMS 437 Medium Impact Cyber Security Policy Appendix A: CIP Exceptional Circumstances Procedure

12.6 RMS 447 Medium Impact Cyber Security Incident Response Plan (CSIRP)

12.7 RMS 432 Physical Access Control System (PACS) Maintenance and Testing Program

12.8 RMS 435 Medium Impact Cyber Security Training and Security Awareness Program