.

Information Type: Confidential
Group Name: The Company, Inc.
Information Owner: Information Security Office

1.1.1.1 Physical Security: Badging Activation – Deactivation Policy

(ISO27001 Policies – SAMPLE DOCUMENT)

Internal Only

.

..

TABLE OF CONTENTS

1 Overview

This Badging Activation Deactivation document describes the policy and processes for enabling Badging stations to provide the physical security badging and access solution at 26 designated site facilities. These are physical site locations that transitioned from the <divestiture>. This policy is identified and organized according to the relevant security controls for physical security in the ISO 27001 specification.

See Appendix C for ISO27001 Annex A.11 Security Controls and Audit, implemented as part of the Information Security Management System (ISMS) for more information.

This Overview describes the following:

- Scope
- Objectives

Each of these sections is described below.

1.1 Scope

The scope of the badging activation ─ deactivation for the sites is to enable authorized personnel (site captains) to activate and deactivate badging and access for people working at, or visiting, a designated facility.

Badging activation and deactivation protects people working at each of the designated facilities against unauthorized intrusion. This includes all employees, contractors, vendors, associates, business partners, third-party vendors, and other responsible parties who are given access to facilities based on their assigned roles and work requirements.

After the interim badging activation ─ deactivation process for sites is in place. The company intends to begin the implementation of a long-range plan to consolidate all sites into one integrated, connected, highly secure enterprise-wide badging access solution. The design and construction of this long-range solution will be forthcoming.

1.2 Objectives

The objectives of the badging activation ─ deactivation process for the sites is to:

- Activate/Deactivate badging and access to each designated facility to protect the people working at or visiting the facility from unauthorized external and internal intrusion.
- Ensure that the badging access solution protects the confidentiality and privacy of each person working at or visiting a designated facility.

In order to meet these objectives, this document contains:

- The badging classification changes needed to migrate badging operations from legacy control to the companies direction and control.
- The process for the initial configuration, implementation, and startup of the badging access solution.
- The process for the in-production, steady state monitoring and management of the badging access solution, once the initial implementation is completed.

2 Appendix C: ISO27001 Annex A.11 Security Controls and Audit

The objective of ISO27001 Annex A.11 specification is to prevent enable security controls that prevent unauthorised physical access, damage and interference to the organisation's information and information processing facilities. The scope of the Badging Activation – Deactivation Policy is described within the context of Annex A.11.1 and Annex A.11.2, as follows:

- Annex A.11.1 is a security specification for the secure physical and environmental security.
- Annex A.11.2 is a security specification for the physical protection of equipment.

2.1 ISO 27001 Annex A.11.1 Physical and Environmental Security

Secure Physical and Environmental Security controls addresses risk inherent to organizational premises, as stated below. Table 1 Secure Area audit questions define how the security controls for Secure Areas as noted below.

2.2 Secure Areas

The A.11.1 specification secures physical and environmental areas prevent unauthorized physical access, damage, and interference to the organization's information, and its information processing facilities.

The controls are covered under the following titles:

- A.11.1.1 Physical security perimeter
- A.11.1.2 Physical entry controls
- A.11.1.3 Securing offices, rooms, and facilities
- A.11.1.4 Protecting against external and environmental threats
- A.11.1.5 Working in secure areas
- A.11.1.6 Delivery and loading areas

Table 1. Secure Areas audit questions

Sl. No	Question / Control Activities
1	Is there a designated security perimeter?
2	Are sensitive or critical information areas segregated and appropriately controlled?
3	Is there any policy for protecting and monitoring the physical infrastructure assets where business information processing, storage, or distribution is performed?
4	Do secure areas have suitable entry control systems to ensure only authorized personnel have access?
5	Have offices, rooms, and facilities been designed and configured with security in mind?
6	Do processes for maintaining the security exist, such as locking up, clear desks, and so on?
7	How is software delivery controlled?
8	Who checks the packages for a potential hazard before each package is used?
9	Have physical protection measures to prevent natural disasters, malicious attack, or accidents been designed in?
10	Do secure areas exist? Where they do exist, do secure areas have suitable policies and processes?
11	Are the policies and processes enforced and monitored?

Sl. No	Question / Control Activities
12	Are there separate delivery / loading areas?
13	Is access from loading areas isolated from the information processing facilities?
14	Is there an access control available? Who has access to the premises?
15	Are servers located in a secured area? Who has access to the servers?
16	Does the organization have visitors' classification? If yes, what are they?
17	Are the visitors escorted at all times or at only for specific time?
18	Who escorts the visitors?
19	Does the Company provide any badge(s) to its visitors? If yes, are the instructions of 'Do's and Don'ts' given to the visitor at the time when the badge is given to them?
20	Are the visitor's vehicles allowed in the office premises?
21	While returning from the Company, does the personnel escorting the visitor ask/remind the visitor to return the Company visitor badge? If no, then who's responsible for the same?
22	Can business visitors visit the facility without prior registration by the host?
23	How the Company carry out the verification of the business visitor?
24	Does the visitor's host inform/communicate with Security in advance of the actual day of the visit?
25	If the business visitor is bringing in their information processing device(s), is that person permitted to take the device(s) inside the Company premises? If yes, what procedure is followed for registration of the device(s)?
26	If the business visitor needs an internet connection for their handheld devices and information processing devices in the Company premises, does the organization permit the visitor to use an internet connection via the Company network? If no, then what is the workaround for the same?
27	Are the visitors allowed to take the photo/video recordings inside the Company premise? If yes, does it need some approval?
28	In situations where the business visitor is to work from the Company facility for more than two consecutive days continuously, or for a longer period, does the Company need to provide the visitor with an access card?
29	When the access card is provided to business visitors in the situation described in #28, what privileges are provided with the access cards?
30	What are the restrictions imposed for general visitors in the Company?
31	To bring personal visitors inside the organization, is any prior authorization is required?
32	For people coming to an interview at the Company premises, how does the security personnel verify each interviewee?
33	Does the Company have any list of restricted devices that cannot be carried inside the premises by general visitors?
34	For ex-the Company staff members, how does the Company security personnel treat these individuals? What type of security checks applies on them?
35	Are the personal visitors allowed to meet the host beyond a certain point, such as reception, in the organization?
36	In case the general visitor wants to tour the office facility, is any (prior) approval required by the Company? If yes, whose authorization is required?
37	What does the office facilities do to allow the pre-approved general visitor to tour a facility?
38	Are the vendor's personnel allowed to visit the workplace or sensitive areas on their own? If yes, what security checks need to be in place? If no, then whose authorization is required to allow the vendor's personnel access to visit the Company facility?
39	During the vendor's personnel registration procedure at the security desk, is the vendor asked or required to declare all devices or equipment being carried inside the office premises?

Sl. No	Question / Control Activities
40	Is the vendor's baggage is also scanned by the security guard?
41	Are the vendors allowed to connect to the Company network?
42	What ID cards does the Company security personnel request from vendor personnel in order to verify their identity?

2.3 ISO 27001 A.11.2 Equipment

The A.11.2 Equipment specification and audit is needed to ensure the physical protection of eguipment, including badging stations, to prevent loss, damage, theft, or compromise of assets, and interruption to the organization's operations.

Audit questions covered from the following titles:

- A.11.2.1 Equipment siting and protection
- A.11.2.2 Supporting utilities
- A.11.2.3 Cabling security
- A.11.2.4 Equipment maintenance
- A.11.2.5 Removal of assets
- A.11.2.6 Security of equipment and assets off-premises
- A.11.2.7 Secure disposal or re-use of equipment
- A.11.2.8 Unattended user equipment
- A.11.2.9 Clear desk and clear screen policy

Table 2. Equipment audit questions

Sl. No	Question / Control Activities
43	How is equipment sited? Are environmental hazards identified and considered when equipment locations are selected?
44	Are the risks from unauthorized access / passers-by considered when siting equipment?
45	Is there an UPS system or back-up generator in place?
46	What controls are in place in case of a power failure?
47	Have these systems and controls been tested within an appropriate timescale? What is the frequency of testing the same?
48	What controls have been considered and implemented to ensure power, telecommunications, cabling data, or supporting information services are protected from interruption or damage?
49	Is there a rigorous equipment maintenance schedule? Is all equipment covered under a maintenance contract? If so, at what frequency is the renewal carried out? How is the maintenance schedule verified and controlled?
50	Is adequate insurance in place to protect equipment removed from the premises?
51	How is sensitive information securely destroyed?
52	Is there a process controlling how assets are removed from site? Is this process enforced?
53	Are spot checks carried out?
54	What preventive measures are in place for desktop security?
55	Are there any auto log off / auto lock procedures available on servers and desktops?

Sl. No	Question / Control Activities
56	Is there any instance of a physical security lapse earlier?
57	Is the system virus protected?
58	Have the critical data and programs in the computer identified and backed up on a regular basis?
59	Is there a policy covering how information assets can be reused?
60	Where data is wiped, is this properly verified before reuse/disposal?
61	Does the organization have a policy around how unattended equipment should be protected?
62	Are technical controls in place to secure equipment that has been inadvertently left unattended?
63	Is there a clear desk / clear screen policy?
64	Is clear desk / clear screen policy well enforced?

3 References

ISO 27001:2013 References		
Clause/Control Number	**Control Objective**	**Control Description**
A.11.1.1	Physical security perimeter	Security perimeters must be defined and used to protect areas that contain either sensitive or critical information or information processing facilities.
A.11.1.2	Physical entry controls	Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
A.11.1.3	Securing offices, rooms, and facilities	Physical security for offices, rooms, and facilities should be designed and applied.
A.11.1.4	Protecting against external and environmental threats	Physical protection against natural disasters, malicious attack or accidents must be designed and applied.
A.11.1.5	Working in secure areas	Procedures for working in secure areas must be designed and applied.
A.11.1.6	Delivery and loading Areas	Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.
A.11.2.1	Equipment sitting and protection	Equipment should be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
A.11.2.2	Supporting utilities	Equipment must be protected from power failures and other disruptions caused by failures in supporting utilities.
A.11.2.3	Cabling security	Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage.
A.11.2.4	Equipment maintenance	Equipment should be correctly maintained to ensure its continued availability and integrity.
A.11.2.5	Removal of assets	Equipment, information or software must not be taken off-site without prior authorization.
A.11.2.6	Security of equipment and assets off-premises	Security should be applied to off-site equipment taking into account the different risks working outside the organization's premises.
A.11.2.7	Secure disposal or re-use of equipment	All items of equipment containing storage media must be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.
A.11.2.8	Unattended user Equipment	Users must ensure that unattended equipment has appropriate protection.
A.11.2.9	Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities must be adopted.
A.8.1.3	Acceptable use of assets	Rules for the acceptable use of information and of assets associated with information and information processing facilities must be identified, documented and implemented.
A.8.1.4	Return of assets	All employees and external party users must return all the organizational assets in their possession upon termination of their employment, contract or agreement.
A.9.2.1	User registration and	A formal user registration and de-registration process must be

ISO 27001:2013 References		
Clause/Control Number	**Control Objective**	**Control Description**
	de-registration	implemented to enable assignment of access rights.
A.9.2.5	Review of user access rights	Asset owners must review users' access rights at regular intervals.
A.9.2.6	Removal or adjustment of access rights	The access rights of all employees and external party users to information and information processing facilities must be removed upon termination of their employment, contract or agreement, or adjusted upon change.

ISMS Document References		
Document Number	**Document Location**	**Document Description**
ISC_PRC_004	ISMS\Procedures	Visitor Management Procedure
INC_ADMN_PRC_001	NCoRE Version 1.0	Physical Security