FACILITY PHYSICAL SECURITY AND ACCESS CONTROL POLICY

POLICY# OTECH-POL2021-008

FRANK L.G. LUJAN, JR. – CHIEF TECHNOLOGYOFFICER
OFFICE OF TECHNOLOGY, GOVERNMENT OFGUAM
otech.guam.gov

OFFICE OF TECHNOLOGY
GOVERNMENT OF GUAM

AUGUST 30, 2021

Overview

Policy Number:	OTECH-POL2021-008
Title:	Facility Physical Security and Access Control Policy
Purpose:	To define the correct use and management of facility level access controls within the Office of Technology (OTECH) And other Government of Guam facility access controlled areas managed by the OTECH.
Authority:	5 GCA Chapter 1 Article 12.106 (e)
Publication Date:	August 30, 2021
Policy Approval:	Frank L.G. Lujan, Jr. OTECH, Chief Technology Officer (CTO)
Target Audience:	All GovGuam employees, contractors and third party vendors requesting access to controlled areas managed by OTECH.
Contact Details:	**Office of Technology** 211 Aspinall Avenue Hagåtña, Guam 96910 O: 671.635-4500 F: 671.472.9508 otech.guam.gov

Revision History

Date of Change	Responsible	Summary of Change
August 2021	OTECH Systems Support	Draft policy
August 2021	CTO, DPM	Review draft, approve and disseminate
March 2022	OTECH Systems Support	• Add physical access device inventory requirements • Add Review & Internal Audit section
March 2022	CTO OTECH CTO, *Frank LG Lujan, Jr.* Date: March 30, 2022	Review and Approve policy updates for dissemination.
June 2022	OTECH Systems Support	• Update document to include section for Key Inventory, Badge Requirement, Server Lock requirements and Authorized Personnel List. • Update Roles and Responsibilities
June 2022	CTO OTECH CTO, *Frank LG Lujan,Jr.* Date: June 7, 2022	• Review and Approve policy updates for dissemination.
February 2024	OTECH Systems Support	(a) Remove DOB requirement for ID badge (b) Add PIV-I section (c) Add Additional Resources section for PIVI instructions & user agreement forms
March 2024	CTO CTO, *Frank LG Lujan, Jr.* Date: March 1, 2024	Review and approve policy updates for dissemination.

Introduction

To define the correct use and management of facility level access controls within Government of Guam (GovGuam) restricted areas, and to provide a protocol to follow to ensure that the information collected, processed and maintained by the Office of Technology (OTECH) is secured in accordance with applicable agreements and regulations. This policy applies to all access-controlled systems managed and maintained by OTECH.

Employee Identification (ID) Badges

All employees with access to secured areas managed by OTECH shall be issued a Government of Guam Employee Identification (ID) Badge that shall include, at minimum, the individuals full name, official title, issue date and employee photo. Employee ID Badge's shall be issued to new employees within thirty (30) days of employment. Employee IDs shall be returned to the Agency for proper disposal upon an individual's retirement, resignation or termination from the Government of Guam or when detailed or transferred to another Government Agency.

GovGuam ID Badges shall be properly displayed above the waist at all times by employees or representatives on work sites and when conducting official GovGuam business or representing the GovGuam/Agency. When the ID Badge is unable to be displayed due to safety, there is an expectation for it to be readily accessible.

Security Access Card Controls & Procedures

In addition to Employee ID Badges, OTECH has implemented card management and monitoring systems to ensure the appropriate use of standard formatted Security Access Cards (SAC). SACs are used to authorize and control access to the GovGuam Datacenters and secured areas within other GovGuam facilities.

SACs are issued to all GovGuam employees with a valid business need to access secured areas, such as the GovGuam Datacenters, the Department of Revenue and Taxation (DRT) facility, and the Department of Public Health and Social Services (DPHSS) offices. Temporary SACs may be issued to contractors and third parties requiring access to GovGuam controlled areas to perform their official duties. GovGuam contractors and third parties may also request access to the GovGuam Datacenter/s if there is a valid business need – this access requires proper approval and a non-disclosure agreement before request is reviewed and considered.

- SAC privileges are granted to users based on the user's assigned division, title duties and responsibilities
- SAC activity may be audited by OTECH IT support personnel, or the user's immediate supervisor or administrator at any time to ensure the proper usage of the user's accessed areas
- SAC privileges may be downgraded, or removed, at any time at the request of a user's immediate supervisor or administrator; but, it may never be raised above the user's title duties and responsibilities
- Access to highly secured areas may be granted to users who hold management, administrative, or supervisorial positions. Such users may only be granted into highly secured areas within their assigned division

- SAC privileges must be revoked as soon as a user is removed or terminated from the department or reassigned to another division.
- SACs issued to OTECH employees require OTECH Chief Technology Officer approval and a signed Security Access Card (SAC) User Acceptance Agreement.
- SACs issued to non-OTECH GovGuam employees shall follow their respective Agency facility access request policy and submit to OTECH for processing.
- SACs issued to non-OTECH GovGuam employees or third-party vendors or contractors requesting access to a GovGuam datacenter must complete and submit a *GovGuam Datacenter Access Terms and Conditions Privacy & Security Agreement* to OTECH. The request must be approved by the respective Agency Director and the OTECH CTO before access is granted.

Personal Identity Verification – Interoperable (PIV-I) Credential

The PIV-I credential is a standard identity credential for issuance to non-Federal employees that meet government standards and provides digital certificates and a secure multi-factor authentication device in one smart card. As of January 2024, OTECH has executed plans to implement PIV-I credentials to replace the standard employee ID badge and SAC. The PIV-I process entails applicant sponsorship, enrollment, identity proofing, and issuance in line with standards of FIPS 201.

OTECH has adopted the Foundation for Trusted Identity (FTI) Policy and Procedures for Issuance of Government of Guam PIV-I credentials. Such documents are proprietary and confidential and shall only be distributed to approved individuals who partake in the PIV-I process for sponsorship, enrollment and issuance. In addition, PIV-I credentials shall also align with the SAC controls aforementioned.

Visitors

Any individual not directly employed or detailed with the Agency is herein defined as a Visitor. All visitors requesting access to controlled areas must sign in the Agency/Division Visitor's Access Log and be escorted when accessing employee-only areas by an authorized employee at all times. The Agency/Division Visitor's Access Log shall, at a minimum, capture the following:

- Name and organization of the visitor
- Signature of the visitor
- Form of identification
- Date of access
- Time of entry and departure
- Purpose of visit
- Name and organization of person visited

The employee identified as the "Name and organization of person visited" must escort the visitor at all times and shall assume responsibility for their visitor's actions. Visitor access to highly secured areas are strictly prohibited. All visitors shall be required to show a valid form of Government-issued identification before access is granted to the facility.

Additional Requirements for OTECH Visitors

Any individual scheduled to drop-off or pick-up equipment or provide professional or technical service to the facility or system resource shall be considered a "visitor" and shall follow the same guidelines and requirements as all visitors.

GovGuam Information Technology (IT) Clearance

Individuals seeking Information Technology (IT) clearance from the Government of Guam shall not be permitted inside the OTECH facility. The clearing individual shall provide their clearance form and government-issued ID to an OTECH personnel to be photocopied and processed. The individual shall be advised to wait outside the building until the process is complete and documents are returned. If the clearance process cannot be completed within an acceptable time, then the individual shall schedule an appointment to return to the office for their documents.

Controlled Doors

Basic security tenets are applied to all facilities at all points of ingress or egress. External controlled facility doors shall remain closed and locked at all times. Restricted areas where personally identifiable information (PII), SSA-provided data, personal health information (PHI), or Federal Tax Information (FTI) is processed shall have additional security on top of the access-controlled doors. Special security such as security cameras and/or motion sensors shall be applied for restricted or high-risk areas containing sensitive information.

"Tailgating" is strictly prohibited when accessing highly controlled areas. For the purpose of this document, tailgating is defined as a physical security breach in which an unauthorized person gains access to a building or other protected area, usually by waiting for an authorized user to open and pass through a secure entry and then following right behind. All authorized personnel are required to scan their SAC upon entering or exiting secured areas. All unauthorized personnel shall adhere to the "Visitor" guidelines.

Server Locks

Servers containing sensitive information (i.e. PII, FTI, SSA-provided data, Health protected data, etc.) shall apply additional security to safeguard its contents and access to the device itself. Servers can be secured, or locked up, by a variety of methods in order to control access to them. The following methods are acceptable ways to comply with the "locked up" server requirements:

- Secure servers by applying physical protection to the server unit (box) itself, by:
  - Secure lid lock to help prevent physical intrusion into the server
  - Secure drive locks to help prevent access to the floppy drive and/or CD ROM drive
  - Anchor pads or cables to secure the server to the rack/table etc. where it is located to prevent removal of the server
- Secure servers by placing them in a lockable server rack.

GovGuam Datacenter Authorized Access List for OTECH Personnel

The OTECH CTO shall maintain a list of all OTECH personnel authorized to access the GovGuam datacenter and secured facilities. The OTECH Authorized Access List shall include the following:

- Name of employee
- Agency or department name
- Access Level
- Purpose of access
- OTECH CTO Signature and Date of Review and Approval

The OTECH Authorized Access List shall be reviewed and updated annually, on an as needed basis, or if

there is a breach in protocol or procedures. The list shall be reviewed on the first day of each Fiscal Year – 1st of October, or the next business day and shall be completed by December 31st of each year. The GovGuam Datacenter OTECH Authorized Access list shall be reviewed and approved by the OTECH CTO.

GovGuam Datacenter Authorized Access List for non-OTECH Personnel

The OTECH CTO shall maintain a list of all non-OTECH personnel authorized to access the GovGuam datacenter and secured facilities. For the purpose of this document, non-OTECH personnel is defined as an individual not employed or detailed directly under OTECH, which includes non-OTECH GovGuam employees (i.e. Agency Director/Deputy, Administrators or designated facility managers), third-party vendors or contractors, facility maintenance personnel, and resource service providers. All non-government personnel must have a current contract/purchase order and a valid business need to access controlled areas. All non-OTECH personnel shall also acknowledge and submit the *GovGuam Datacenter Access Terms and Conditions Privacy & Security Agreement*.

The GovGuam Datacenter Authorized Access list for non-OTECH personnel shall include the following:

- Name of employee/vendor/contractor/non-agency personnel
- Agency or department name
- Name, phone number and email of the Agency POC authorizing access
- Address if agency/vendor/contractor
- Purpose and level of access
- OTECH CTO Signature and Date of Review and Approval

The non-OTECH Personnel Authorized Access List shall be reviewed and updated annually, on an as needed basis, or if there is a breach in protocol or procedures. The list shall be reviewed on the first day of each Fiscal Year – 1st of October, or the next business day and shall be completed by December 31st of each year. The GovGuam Datacenter Authorized Access list for non-OTECH personnel shall be reviewed and approved by the OTECH CTO.

GovGuam Datacenter Physical Inventory Guidelines

OTECH shall ensure control of all access points to GovGuam datacenters managed, maintained and supported by OTECH. Entry door keys, server rack cabinet keys and safe combinations shall be safeguarded and maintained by OTECH personnel with administrative or management roles and shall be inventoried annually (January of each year) and changed any time the keys are lost, combinations are compromised, or individuals are terminated or transferred. The primary set of keys shall be safeguarded in a secured, locked area only known by the OTECH CTO and Data Processing Manager (DPM); the secondary set of keys shall be safeguarded in a secured, locked area only know by the OTECH Operations Manager.

Internal audits for access to GovGuam datacenters shall follow the OTECH-SOP2019-001 *Internal Audit and Accountability Review for GovGuam Datacenter Facilities* SOP document.

Review and Internal Audit

This policy shall be reviewed and updated annually, on an as needed basis, or if there is a breach in protocol and procedures. OTECH shall initiate the review process on the first day of each Fiscal Year – 1st of October, or next business day. Policy review and updates shall be documented in the policy's *Revision History* section. The review process shall be completed before the end of the Fiscal Year's first quarter

and the updated policy shall be disseminated (via OTECH website, Agency Memo or email) by December 31 of each year.

Roles & Responsibilities

Role	Responsibility
OTECH Chief Technology Officer (CTO)	• Overall responsibility for the security, functionality and support of the security access card systems • Overall responsibility for reviewing and updating the technical aspect of this policy on an annual or as needed basis • Overall responsibility for reviewing and approving the OTECH Authorized Access List and Non-OTECH Authorized Access List as required by this document • Overall responsibility to ensure that all OTECH employees, third party vendors, contractors and visitors comply with this policy • Ensure this policy is updated on an annual or as needed basis
OTECH Data Processing Manager (DPM)	• Overall responsibility for supporting the CTO on management roles in accordance to this policy and all other applicable IT policies and procedures
OTECH Operations Supervisor	• Overall responsibility to safeguarding all secondary keys to secured areas and network resources
OTECH System Administrator (SA)	The System Administrator (SA) is appointed by the OTECH CTO and is responsible for: • Managing the access card system • Maintaining access card request forms and logs • Ensuring that access card request forms are made available for review to the appropriate personnel • Ensuring the access card system is operational and all backups are successful and retained • Creating new sites and access levels as needed • Generating access card activity reports as needed • Creating and maintaining a diagram of all access controls • Recommending security enhancements to the OTECH CTO • Tracking which staff have access to the building and ensure access is appropriate for staff respective duties • Reporting all security card access equipment issues to the SA • Review Access Control logs on a quarterly basis to establish baselines, identify operational trends, identify failed login attempts and support internal investigations • Review physical access logs on a quarterly basis and compare with access control logs to ensure that access control policies are being adhered to. • Engaging with access control vendor support to troubleshoot any issues with access control equipment • Taking prompt and proper action on receipt of access request forms for access card activation, updates, or deactivation

	• Logging all completed access card requests • Investigating SACs inactive for ninety (90) or more days to determine if card should be disabled
Agency Heads	• Overall responsibility for supporting OTECH on implementing and adhering to the guidelines of this policy and all other applicable IT policies and procedures • Overall responsibility for ensuring that budget is properly allocated for security systems and supplies deployed at their respective Agency facilities • Ensure all staff members acknowledge and understand the terms of this policy and all other applicable IT policies and procedures • Take prompt and proper measures to review and approve each Facility Access Request, ensuring that all access is requested based the user's role and responsibility • Create and maintain an Agency level Facility Access Policy that governs the Agency's internal procedures on requesting, approving and deactivating facility access accounts
Agency Division/Bureau Administrators or Supervisors	• Ensure that all personnel who report to them are notified and instructed to comply with this policy • Take prompt and proper measures to ensure that they complete the required access card request form on behalf of all personnel who report to them • Ensure that all request forms are completed and submitted on a timely matter, for both permanent and temporary staff, allowing ample time for the activation, updating, or deactivation of an access card prior to a user's start, end or suspension date • Ensure that each user they request access for is based on their title responsibilities and duties • Report any misuse or abuse of access card privileges to the OTECH CTO, DMP or SA • Comply to the terms of this policy
Employees	• Comply with the terms of this policy • Notify their supervisor or administrator immediately when their access card is lost or damaged • Surrender access card upon termination of Government of Guam employment • Report any misuse or abuse of access card privileges to their immediate • supervisor or administrator

Additional Resouces

- OTECH 24-001 (Sponsor PIV-I request) – Instructions
- OTECH 24-002 (PIV-I Enrollment & Issuance Check List and User Acknowledgement

Security Access Card (SAC) User Acceptance Agreement

This agreement outlines the responsibilities I have as a holder of a Government of Guam Security Access Card (SAC). My acceptance of this agreement indicates that I have read and understand these responsibilities, and agree to adhere to the protocol and procedures established for Security Access Cards.

1. The SAC is intended to facilitate the entry to electronically access-controlled doors within GovGuam restricted facilities managed by the Office of Technology (OTECH)
2. The SAC is issued in my name as the sole authorized person for access to the appropriate areas. I will not allow any other person to use my SAC. I understand that OTECH records and maintains data regarding my personal use of my SAC.
3. Duplication of my SAC or unauthorized use the SAC including permitting others to gain authorized access to restricted or high-risk areas is considered misappropriation of access privileges. This could result in immediate and irrevocable forfeiture of the SAC and/or access privileges to electronically access-controlled area.
4. I understand that the SAC is the property of GovGuam and must be surrendered upon leaving OTECH or issuing Agency, whether for transfer, termination or dismissal. I may also be requested to surrender the SAC for reasons not related to my own personal situation.
5. I will maintain the SAC appropriate security whenever and wherever I use the SAC. I will not tamper or intentionally damage the SAC in any way, shape or form. I will take all reasonable care to prevent the SAC from being damaged, lost, stolen or misused. If the SAC is lost or stolen, I agree to immediately notify my immediate supervisor or administrator.
6. I will notify my immediate supervisor or administrator regarding any unauthorized use of the SAC.

Conditions of Issue

The Security Access Card (SAC) is issued to you, with the written approval of your supervisor and administrator, as evidence of your need to access electronically access-controlled areas.

You must not lend your SAC to anyone to allow them to gain unauthorized access to Government of Guam facilities. You may be subject to a replacement fee, payable to the Treasurer of Guam, if your card is lost, stolen or defaced.

The Security Access Card (SAC) remains the property of GovGuam at all times.

OTECH or issuing Agency reserves the right to withdraw from an individual, any or all the facilities of the SAC and request that the SAC be surrendered, if evidence is found that the SAC is being misused in any way. Any unauthorized use of the SAC or violation of this policy may result in confiscation of the SAC and/or disciplinary action, including termination and prosecution.

Acknowledgment

I acknowledge that I have read, understood and agree to this policy.

User Full Name _____

Agency/Company _____

Position/Title _____

User Signature _____ Date _____

Director Signature _____ Date _____