

USER ACCESS & CONTROL MANAGEMENT POLICY

POLICY# OTECH-POL2020-002

FRANK L.G. LUJAN, JR. – CHIEF TECHNOLOGY OFFICER
OFFICE OF TECHNOLOGY, GOVERNMENT OF GUAM
Otech.guam.gov

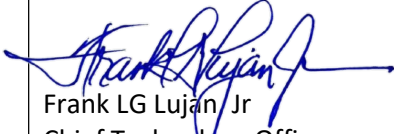


OFFICE OF TECHNOLOGY
GOVERNMENT OF GUAM

MARCH 4, 2020



Overview

Policy Number:	OTECH-POL2020-002
Title:	User Access & Control Management Policy
Purpose:	To establish adequate controls to Government of Guam Information Technology (IT) systems and devices maintained by the Office of Technology (OTECH).
Authority:	5 GCA Chapter 1 Article 12.106 (e)
Publication Date:	March 4, 2020
Policy Approval:	 Frank LG Lujan Jr Chief Technology Officer
Target Audience:	All OTECH employees, contractors, vendors and third parties. The intended recipients of this policy also include all entities under the authority of the Office of Technology, pursuant to the provisions of Public Law 34-076.
Contact Details:	Office of Technology 211 Aspinall Avenue PO Box 884 Hagåtña, Guam 96910 O: 671.635.4500 F: 671.472.9508 otech.guam.gov



Revision History

Date of Change	Responsible	Summary of Change
October 2018	OTECH Systems Support	Draft policy
February, March, July, December 2019	OTECH Systems Support	Update Policy and Format
March 2020	OTECH CTO and Data Processing Manager	Review, approve and disseminate policy



Introduction

Information security is the protection of information against accidental or malicious disclosure, modification or destruction. Information is an important, valuable asset of the Government of Guam's Information Technology systems which must be managed with care.

The Office of Technology (OTECH) is committed to ensuring the security and confidentiality of the information it processes on behalf of the Government of Guam (GovGuam). Poor management of access controls to sensitive information processed and stored within GovGuam facilities can lead to the illicit act of disclosure of information, fraud, and possible lawsuits.

This policy is intended to define the appropriate use and management of user level access controls to GovGuam Applications, Systems and Devices managed and maintained by OTECH, as well as to harden and mature our collective efforts in improving our overall cybersecurity posture. Access to GovGuam information systems must be restricted to only authorized users or processes, based on the principal of strict need to know and least privilege.

Definitions

Access Control – the process that limits and controls access to information technology resources.

Access Privileges – system permissions associated with an account, including permissions to access or change data, to process transactions, create or change settings, etc.

Cyber Incident/Cyber Breach - An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or that constitutes a violation or imminent threat of violating security policies, security procedures, or acceptable use policies.

Cybersecurity - An approach or series of steps to prevent or manage the risk of damage to, unauthorized use of, exploitation of, and—if needed—to restore electronic information and communications systems, and the information they contain, in order to strengthen the confidentiality, integrity, and availability of these systems.

Non-disclosure Agreement – a contract between a person and an Institution stating that the person will protect confidential information covered by the contract, when this person has been exposed to such information.

Privileged Accounts – system or application accounts that have advanced permissions (as compared to regular user account permissions) on GovGuam systems and applications.

Users – are GovGuam employees, consultants, contractors, agents, vendors and authorized users accessing GovGuam Information Technology resources (i.e. systems, applications, infrastructure, etc.).

1.0 Policy

1.1 Principles of Access Control

Access privileges to GovGuam information systems are based on the following principles:



- Need to know – users or resources will be granted access to systems that are necessary to fulfill their roles and responsibilities.
- Least privilege – users or resources will be provided with the minimum privileges necessary to fulfill their roles and responsibilities.

1.2 General Account Requirements

- Requests for users' accounts and access privileges must be formally documented and appropriately approved.
- User accounts are to be provisioned (created, updated, or deactivated) by the IT Administrator. User account requests requiring specific access may be forwarded to the Application Administrator for provisioning.
- Requests for special accounts and privileges (such as supervisor and administrator access, remote access and test accounts) must be formally documented and appropriately approved.
- Application accounts must only be used by application components requiring authentication; access to the account settings must be restricted to authorized IT Administrators, Application Administrators and application developers only.
- Where possible, OTECH will set user accounts to automatically expire at a pre-set date. More specifically,
 - When temporary access is required, such access will be removed immediately after the user has completed the task for which the access was granted.
 - User accounts assigned to contracts, vendors or third parties will be set to expire according to the contract's expiry date.
 - User accounts will be disabled after 60 days of inactivity.
- Access rights will be immediately disabled or removed when the user is terminated or ceases to have a legitimate reason to access GovGuam systems.
- A verification of the user's identity must be performed by the IT Administrator, Application Administrator, IT Help Desk, or designate before enabling or resetting a password.
- Existing user accounts and access rights will be reviewed at least annually to detect dormant accounts and accounts with excessive privileges. Annual reviews will be conducted by the Agency/Division heads overseeing the operations of their respective information technology system, their respective application vendor support or their IT



Analyst. Annual reviews must be scheduled with the IT Administrator. Examples of excessive privileges include:

- An active account assigned to external contractors, vendors or employees that no longer work for the Agency.
- An active account with access rights for which the user's role and responsibilities do not require access.
- Unknown active accounts.

1.3 Shared User Accounts

- Where possible, the use of specific network domain "security groups" should be used to share common access permissions across many users, instead of shared accounts.
- Shared user account are only to be used on an exception basis with the appropriate approval. Examples of shared accounts may be used on customer counter workstations. Access to the workstation may be shared, but access to specific applications must be controlled using the individual's assigned and approved user account.

1.4 Vendor or Default User Accounts

- Where possible, all default user accounts will be disabled or changed. These accounts include "guest", "temp", "admin", "Administrator", and any other commonly known or used default accounts, as well as related default passwords used by vendors on "commercial off-the shelf" systems and applications.

1.5 Test Accounts

- Test accounts can only be created if they are justified by the relevant business area or management team and appropriately approved.
- Test accounts must have an expiry date (maximum of 6 months). Maintaining test accounts beyond this date must be re-evaluated every 90 days and approved appropriately.
- Test accounts will be disabled when they are no longer necessary.

1.6 Contractors and Vendors

- Contract with contractors/vendors will include specific requirements for the protection of data. In addition, contractor/vendor representatives accessing information systems with sensitive data (i.e. systems with Personally Identifiable Information (PII) or medical or health information (protected by HIPPA)) will be required to sign a Non-disclosure Agreement ("NDA") prior to obtaining approval to access GovGuam systems and applications.



- Prior to granting access rights to a contractor/vendor, the OTECH Chief Technology Officer (CTO) or IT Administrator must verify the NDA and protection of data requirements have been complied with.
- The name of the contractor/vendor representative must be communicated to the IT Help Desk at least 2 business days before the person needs access.
- The need to terminate the access privileges of the contractor/vendor must be communicated to the CTO, IT Administrator or Help Desk at least 1 business day before the contractor/vendor representative's need for such access ends.

1.7 Access Control Requirements

- All users must use a unique ID to access GovGuam systems and applications. Passwords must be set in accordance with the OTECH Password Policy.
- Alternative authentication mechanisms that do not rely on a unique ID and password must be formally approved by the CTO and/or IT Administrator.

Request Forms

- OTECH 19-005 (Active Directory & Email Request) - <https://otech.quam.gov/resources/>
- OTECH 19-005 (Attachment for Multiple User Request) – <https://otech.quam.gov/resources/>
- OTECH 19-008 (Elevated Privileges Rules of Behavior & Security Agreement) - <https://otech.quam.gov/resources/>
- Application & System Request Forms – *refer to respective Agency Admin Office*

Roles & Responsibilities

Role	Responsibility
OTECH Chief Technology Officer (CTO)	<ul style="list-style-type: none">• Overall responsibility for the security, functionality and support of the user access and control of all GovGuam information systems, resources and applications supported and maintained by OTECH• Overall responsibility for reviewing and updating this policy on an annual or as needed basis• Review all vendor and contractor user access requests forms comply to the requirements of this policy
Agency Heads	<ul style="list-style-type: none">• Overall responsibility to ensure that all their employees, third party vendors and contractors comply with this policy• Ensure this policy is updated on an annual or as needed basis• Support the OTECH CTO with new security implementations and protocols pertaining to this policy• Review and explicitly approve or disapprove any exceptions to the requirements of this policy• Review and explicitly approve or disapprove user access requests• Review all vendor and contractor user access requests forms comply to the requirements of this policy



IT Administrator	<p>The IT Administrator for each Agency may vary, is appointed by the OTECH CTO and is responsible for:</p> <ul style="list-style-type: none">• Complying with the terms of this policy and all other relevant OTECH policies, procedures, regulations and applicable legislations• Taking prompt and proper action on receipt of user and access request forms in accordance with this policy• Notifying users of their system account details in a secure and confidential manner• Recommending security enhancements to the OTECH CTO
Application Administrator	<p>The Application Administrator for each Agency and Application may vary:</p> <ul style="list-style-type: none">• Complying with the terms of this policy and all other relevant OTECH policies, procedures, regulations and applicable legislations• Taking prompt and proper action on receipt of user and access request forms in accordance with this policy• Notifying users of their system account details in a secure and confidential manner• Recommending security enhancements to the IT Administrator and OTECH CTO
IT Help Desk	<p>The IT Help Desk is operated by the Office of Technology and is responsible for:</p> <ul style="list-style-type: none">• Complying with the terms of this policy and all other relevant OTECH and GovGuam policies, procedures, regulations and applicable legislations• Supporting the IT Administrator and CTO on their duties and responsibilities in accordance to the terms of this policy
Agency Branch/Division /Bureau Administrators	<ul style="list-style-type: none">• Disseminate and implement this policy within their respective division/branch/bureau• 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 user access request form(s) 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 disabling of an access account prior to a user's start, end or suspension date• Immediately notify the IT Administrator of any changes in personnel and access control requirements• Ensure that each user they request access for is based on their title responsibilities and duties• Report any misuse or abuse of access to the Agency heads and respective IT Administrator/Contact• Comply to the terms of this policy
Employees	<ul style="list-style-type: none">• Comply with the terms of this policy• Report all non-compliance instances with this policy (observer or suspected) to their Supervisor or Administrator as soon as possible.



Policy Compliance

Compliance Measurement

The Office of Technology will verify compliance to this policy through various methods, including but not limited to periodic reviews and site inspections, video monitoring, business tool reports, internal and external audits and inspections, and feedback from any and all other sources.

Exceptions

Exceptions to the guiding principles in this policy must be documented and formally approved by the requestor's respective Supervisor, Agency Head and the Chief Technology Officer (CTO).

Policy exceptions must describe:

- The nature of the exception
- A reasonable explanation for why the policy exception is required
- Any risks created by the policy exception
- Evidence of approval by all appropriate parties

Non-Compliance

Any user found to have violated this policy may have his/her privileges revoked and may be subject to disciplinary and/or legal action. The unauthorized use of any form of hacking programs or tools within the confines of the GGWAN or any GovGuam networked device is strictly prohibited. Any violations will be considered a cyber incident or cyber breach and will be prosecuted to the fullest extent of the laws of the territory of Guam.