INFORMATION SECURITY POLICY

Public Version

Table of Contents

1 Version Control

VERSION	DATE	MADE BY	VERIFIED BY	APPROVED BY	COMMENTS
1.0	05/27 /2022	Ing. Cleyderman Guerrero	Ing. Omar Arvelo		Map CSF
2.0	07/25/2022	Ing. Cleyderman Guerrero	Ing. Omar Arvelo		Map CSF
3.0	10/25/2022	Ing. Cleyderman Guerrero	Ing. Omar Arvelo		Map CSF NIST
4.0	01/18/2023	Bruno Oliveira (Protiviti Inc)	Ing. Omar Arvelo	Marcelo Del Vigna (Legal)	Map CSF NIST

2 Purpose

This policy defines the mandatory minimum information security requirements for GlobeNet as defined below in Section 3 Scope. GlobeNet may, based on its individual business needs and specific legal and federal requirements, exceed the security requirements put forth in this document, but must, at a minimum, achieve the security levels required by this policy.

This policy acts as an umbrella document to all other security policies and associated standards. This policy defines the responsibility to:

- protect and maintain the confidentiality, integrity and availability of information and related infrastructure assets;
- manage the risk of security exposure or compromise;
- assure a secure and stable information technology (IT) environment;
- identify and respond to events involving information asset misuse, loss, or unauthorized disclosure;
- monitor systems for anomalies that might indicate compromise; and
- promote and increase the awareness of information security.

This policy benefits GlobeNet by defining a framework that will assure appropriate measures are in place to protect the confidentiality, integrity, and availability of data; and assure staff and all other affiliates understand their role and responsibilities, have adequate knowledge of security policy, procedures and practices and know how to protect information.

3 Scope

This Policy applies to all GlobeNet's computer systems and facilities, including those managed on GlobeNet's behalf by third parties. This Policy applies to all employees, partners and third parties with access to GlobeNet's Technology Assets. Technology Assets and the information resident on them are the property of GlobeNet.

Violations to this Policy may be subject to disciplinary action up to and including termination of employment. In addition, when circumstances warrant, breaches of security and failure to comply with this Policy will be referred to external law enforcement when appropriate. Users who discover a violation of this Policy must promptly notify their manager, Human Resources or the Help Desk. Business partners and managed service providers should report any violation of this Policy to their designated point of contact.

Furthermore, this Policy addresses the roles, responsibilities, security best practices, enforcement, and acceptable and unacceptable use of Technology Assets, which include but are not limited to:

- Bluetooth
- Cameras
- Data
- Email
- External drives
- Freeware/Shareware
- Internet
- Internet storage
- Network
- Message boards and blogs
- Passwords
- Password cracking software
- Personal Information
- Phones
- Physical security
- Printers
- Remote access
- Scanners
- Social Networks
- USB drives
- Wireless devices.

4 Information Statement

4.1. Organizational Security

Information security requires both an information risk management function and an information technology security function. Depending on GlobeNet's structure, such functions may be performed separately by different individuals, groups, or performed jointly by the same individual or group. These functions must be performed by a high-level executive or a group that includes high level executives.

1. GlobeNet must designate an individual or group to be responsible for the risk management function assuring that:
   a. risk-related considerations for information assets and individual information systems, including authorization decisions, are viewed as an enterprise with regard to the overall strategic goals and objectives of carrying out its core missions and business functions; and

   b. the management of information assets and information system-related security risks is consistent, reflects the risk tolerance, and is considered along with other types of risks, to ensure mission/business success.

2. GlobeNet must designate an individual or group to be responsible for the technical information security function. For purposes of clarity and readability, this policy will refer to the individual, or group, designated as the Information Security Officer (ISO)/designated security representative. This function will be responsible for evaluating and advising on information security risks.

   a. Information security risk decisions must be made through consultation with both function areas described in a. above.

b. Although the technical information security function may be outsourced to third parties, GlobeNet retains overall responsibility for the security of the information that it owns.

4.2. Functional Responsibilities

1. IT Team is responsible for:

   a. supporting security by providing clear direction and consideration of security controls in the data processing infrastructure and computing network(s) which support the information owners;
   b. providing resources needed to maintain a level of information security control consistent with this policy;
   c. identifying and implementing all processes, policies and controls relative to security requirements defined by the business and this policy;
   d. implementing the proper controls for information owned based on the classification designations;
   e. providing training to appropriate technical staff on secure operations (e.g., secure coding, secure configuration);
   f. fostering the participation of information security and technical staff in protecting information assets, and in identifying, selecting and implementing appropriate and cost-effective security controls and procedures; and
   g. implementing business continuity and disaster recovery plans.

2. The workforce (including: Employees, Contractors, Consultants and Third-Party Vendors) is responsible for:

   a. keeping up to date with this policy and related procedures and standards, understanding the baseline information security controls necessary to protect the confidentiality, integrity and availability of information entrusted;
   b. protecting information and resources from unauthorized use or disclosure;
   c. protecting personal, private, sensitive information from unauthorized use or disclosure;
   d. abiding by *Acceptable Use of Information Technology Resources Policy*
   e. Referencing this policy and related procedures and standards, and reporting suspected information security events, incidents or weaknesses to your manager and ISO/designated information security representative.
   f. in the case of employees occupying a strategic and/or executive position at GlobeNet:

      i. ensure compliance with this policy by their subordinates;
      ii. evaluating and accepting risk on behalf of GlobeNet;
      iii. identifying information security responsibilities and goals and integrating them into relevant processes;
      iv. supporting the consistent implementation of information security policies and standards;

v. supporting security through clear direction and demonstrated commitment of appropriate resources;

vi. promoting awareness of information security best practices through the regular dissemination of materials provided by the ISO/designated information security representative;

vii. implementing the process for determining information classification and categorization, based on industry recommended practices, organization directives, and legal and regulatory requirements, to determine the appropriate levels of protection for that information;

viii. implementing the process for information asset identification, handling, use, transmission, and disposal based on information classification and categorization;

ix. determining who will be assigned and serve as information owners while maintaining ultimate responsibility for the confidentiality, integrity, and availability of the data;

x. participating in the response to security incidents;

xi. complying with notification requirements in the event of a breach of private information;

xii. adhering to specific legal and regulatory requirements related to information security;

xiii. communicating legal and regulatory requirements to the ISO/designated security representative; and

xiv. communicating requirements of this policy and the associated standards, including the consequences of non-compliance, to the workforce and third parties, and addressing adherence in third party agreements.

3. The Cybersecurity Team is responsible for:

a. providing in-house expertise as security consultants as needed;
b. developing the security program and strategy, including measures of effectiveness;
c. establishing and maintaining enterprise information security policy and standards;
d. assessing compliance with security policies and standards;
e. advising on secure system engineering;
f. providing incident response coordination and expertise;
g. monitoring networks for anomalies;
h. monitoring external sources for indications of data breaches, defacements, etc.
i. maintaining ongoing contact with security groups/associations and relevant authorities;
j. providing timely notification of current threats and vulnerabilities; and
k. providing awareness materials and training resources.
l. maintaining familiarity with business functions and requirements;
m. maintaining an adequate level of current knowledge and proficiency in information security through annual Continuing Professional Education (CPE) credits directly related to information security;
n. assessing compliance with information security policies and legal and regulatory information security requirements;

o. evaluating and understanding information security risks and how to appropriately manage those risks;
p. representing and assuring security architecture considerations are addressed;
q. advising on security issues related to procurement of products and services;
r. escalating security concerns that are not being adequately addressed according to the applicable reporting and escalation procedures;
s. disseminating threat information to appropriate parties;
t. participating in the response to potential security incidents;
u. participating in the development of enterprise policies and standards that considers GlobeNet’s needs; and
v. promoting information security awareness

4.3. Segregation of Duties

1. To reduce the risk of accidental or deliberate system misuse, separation of duties and areas of responsibility must be implemented where appropriate.

2. Whenever separation of duties is not technically feasible, other compensatory controls must be implemented, such as monitoring of activities, audit trails and management supervision.

3. The audit and approval of security controls must always remain independent and segregated from the implementation of security controls.

4.4. Risk Management

GlobeNet must ensure that risk management processes are managed and agreed with the Organization's strategy, observing regulatory, legal, environmental, technological, and operational requirements. For that it shall:

1. Consider vulnerabilities, threat sources, and security controls that are planned or in place to proper Information security risk management.

2. Develop, document, and maintain risk management processes and regularly review to ensure they remain effective and relevant and that all stakeholders are aware of their responsibilities and the steps to be taken to protect the organization's information and assets.

3. **The risk management process is iterative and should be followed throughout a system’s or process’s life cycle.**

4. Monitor the effectiveness of its risk response measures, by verifying that the controls put in place are implemented correctly and operating as intended. **This must occur annually, at a minimum.**

5. Manager appropriately any system or process that supports business functions for information risk and undergo information risk assessments, at a minimum annually, as part of a system life cycle.

6. Require Information security risk assessments for any new projects, implementations of new technologies, significant changes to the operating environment, or in response to the discovery of a significant vulnerability.

7. Select the risk assessment approach it will use based on its needs, applicable laws and regulations as well as applicable policies.

8. Document all risk assessment results, and the decisions made based on these results to support further reviews and other related actions.

4.5. Vendor Risk Management

In order to identify, assess and mitigate risks that may arise from the use of external third parties, such as suppliers, contractors and service providers, GlobeNet must protect its assets, reputation and compliance posture, ensuring that third parties comply with the organization's policies and standards, as well as relevant laws and regulations. To do so, it must:

1. Identify third parties that pose a potential risk to the organization.

2. Evaluate the risks associated with each third party, taking into account factors such as the sensitivity of the data processed, the nature of the services provided and the geographic location of the third party.

3. Perform due diligence on third parties and suppliers before entering into a relationship with them, in order to identify potential risks, including assessing information security maturity and allowing the organization to mitigate them.

4. Specific provisions related to information security, privacy of personal data and other protection mechanisms must be included in contracts with third parties and suppliers, in order to manage the risks associated with the relationship with GlobeNet. Where applicable, service contracts shall require the third party or vendor to maintain insurance coverage.

5. Monitor the performance of third parties to ensure they are in compliance with the organization's policies and standards and identify potential risks and allow GlobeNet to take timely measures to mitigate them.

6. Establish clear lines of communication and procedures to escalate issues to stakeholders to ensure risks are identified and addressed in a timely manner.

7. Contract clauses must be included that allow GlobeNet to immediately terminate the relationship with a third party or supplier in the event of a breach or other event related to information security.

4.6. Asset Management

GlobeNet must ensure that Information Technology (IT) resources are inventoried and configured in compliance with this information security policies and other standards and procedures. In this case it shall:

1. Develop, document, and maintain under configuration control, a current baseline configuration of information systems.

2. Review and update the baseline configuration of the information system when required and as an integral part of information system component installations and upgrades. Periodic review must occur annually, at a minimum.

3. Develop, document, and maintain a configuration change control process to determine the types of changes to the information system that are configuration-controlled.

4. Develop, document, and maintain a security impact analysis process to analyze changes to the information system to determine potential security impacts prior to change implementation.

5. Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.

6. Establish and document configuration settings for information technology products employed within the information system that reflect the most restrictive mode consistent with operational requirements.

7. Monitor and control changes to the configuration settings in accordance with policies and procedures.

8. Configure the information system to provide only essential capabilities.

9. Review the information system periodically to identify unnecessary and/or unsecure functions, ports, protocols and services.

10. Review and update the list of unauthorized software programs annually.

11. Develop and document an inventory of information system components that:

    a. Reflects the current information system accurately.
    b. Includes all components within the authorization boundary of the information system.
    c. Is at the level of granularity deemed necessary for tracking and reporting.
    d. Includes information deemed necessary to achieve effective information system component accountability.

12. Review and update the information system component inventory when necessary and/or periodically. Periodic review must occur every 2 years, at a minimum.

13. Update the inventory of information system components as an integral part of component installations, removals, and information system updates.

14. Employ automated mechanisms, including regular scanning, to detect the presence of unauthorized hardware, software, and firmware components within the information system.

15. Disposal of IT assets must be carried out properly when they are no longer needed or when they have reached the end of their useful life, in order not to discard information belonging to GlobeNet together with said assets.

4.7. Acceptable Use of Information Technology

GlobeNet advises that the appropriate organizational use of information and its information technology ("IT") resources and the effective security of these resources requires the participation and support of the organization's workforce ("users"). Improper use exposes the organization to potential risks, including virus attacks, compromised systems and network services, and legal issues.

All uses of information and information technology resources must comply with GlobeNet´s policies, standards, procedures, and guidelines, as well as any applicable license agreements and laws including Federal, State, local and intellectual property laws.

Consistent with the foregoing, the acceptable use of information and IT resources encompasses the following duties:

1. Understanding the baseline information security controls necessary to protect the confidentiality, integrity, and availability of information;
2. Protecting organizational information and resources from unauthorized use or disclosure;
3. Protecting personal, private, sensitive, or confidential information from unauthorized use or disclosure;
4. Observing authorized levels of access and utilizing only approved IT technology devices or services; and
5. Immediately reporting suspected information security incidents or weaknesses to the appropriate manager and the Information Security Officer (ISO)/designated security representative.

Reinforcing the commitment to the proper use of GlobeNet's information technology resources, the following is considered **unacceptable use**:

6. Unauthorized use or disclosure of personal, private, sensitive, and/or confidential information;
7. Unauthorized use or disclosure of GlobeNet's information and resources;
8. Distributing, transmitting, posting, or storing any electronic communications, material or correspondence that is threatening, obscene, harassing, pornographic, offensive, defamatory, discriminatory, inflammatory, illegal, or intentionally false or inaccurate;
9. Attempting to represent the organization in matters unrelated to official authorized job duties or responsibilities;
10. Connecting and using personal owned or unapproved devices to the organization's network or any IT resource;

11. Connecting organizational IT resources to unauthorized networks;

12. In case of using remote access:

    a. Connecting to any wireless network while physically connected to the organization's wired network;

    b. Installing, downloading, or running software that has not been approved following appropriate security, legal, and/or IT review in accordance with organizational policies;

13. Using an organization's IT resources to circulate unauthorized solicitations or advertisements for non-organizational purposes including religious, political, or not-for-profit entities;

14. Providing unauthorized third parties, including family and friends, access to the organization's IT information, resources or facilities;

15. Using organization IT resources for commercial or personal purposes, linked with "for-profit" activities or supporting alien business activity (e.g., consulting for pay, business transactions);

16. Propagating chain letters, fraudulent mass mailings, spam, or other types of undesirable and unwanted email content using organizational IT resources; and

17. Tampering, disengaging, or otherwise circumventing any GlobeNet or third-party IT security controls.

Other actions should be considered to ensure security and compliance regarding the use of GlobeNet's IT resources, such as:

18. Individual accountability is required when accessing all IT resources and organization information. Everyone is responsible for protecting against unauthorized activities performed under their user ID. This includes locking your computer screen when you walk away from your system, and protecting your credentials (e.g., passwords, tokens or similar technology) from unauthorized disclosure. Credentials must be treated as confidential information and must not be disclosed or shared.

19. Users must not transmit restricted organization, non-public, personal, private, sensitive, or confidential information to or from personal email accounts (e.g., Gmail, Hotmail, Yahoo) or use a personal email account to conduct the organization's business unless explicitly authorized. Users must only store restricted organizational, non-public, personal, private, sensitive, or confidential information on an organizational issued device, or with a third-party file storage service that has been approved for such storage by the organization.

20. Devices that contain organizational information must be always attended or physically secured and must not be checked in transportation carrier luggage systems.

21. Users are routinely assigned or given access to IT equipment in connection with their official duties. This equipment belongs to the organization and must be immediately returned upon request or at the time an employee is separated from the organization. Users may be financially responsible for

the value of equipment assigned to their care if it is not returned to the organization. Should IT equipment be lost, stolen or destroyed, users are required to provide a written report of the circumstances surrounding the incident. Users may be subject to disciplinary action which may include repayment of the replacement value of the equipment. The organization has the discretion to not issue or re-issue IT devices and equipment to users who repeatedly lose or damage IT equipment.

22. In instances where users access social media sites on their own time utilizing personal resources, they must remain sensitive to expectations that they will conduct themselves in a responsible, professional, and secure manner regarding references to GlobeNet and staff.

23. Users should respect the privacy of the organization’s staff and not post any identifying information of any staff without permission (including, but not limited to, names, addresses, photos, videos, email addresses, and phone numbers). Users may be held liable for comments posted on social media sites.

24. Users are strongly discouraged from using the same passwords in their personal use of social media sites as those used on GlobeNet devices and IT resources, to prevent unauthorized access to resources if the password is compromised.

25. For cases where there is use of social media within the scope of official duties, the accounts used to manage GlobeNet's presence on social media are privileged accounts and must be treated as such. These accounts are for official use only and should not be used for personal use. Privileged account passwords must follow information security standards, be unique on each site, and must not be the same as passwords used to access other IT resources.

4.8. Account Management and Access Control

1. All employee account creation requests are to be submitted via a Help Desk ticket. The request must contain the employee’s full name, company/division, department, job title, manager, and any special authorizations, such as access to certain applications. If the request requires any application or special group access, the Help Desk will forward the ticket to the appropriate Business Administrator. The Business Administrator will approve the request.

2. All vendor’s account creation requests are to be submitted via a Help Desk ticket from the manager of the department that has the vendor relationship. This request must have (i) the request type, (ii) vendor’s name, (iii) the reason for the requested access, (iv) specific resources needed, and (v) contact information. *[Internal and Confidential Information]*

3. If the new account is related to a new GlobeNet’s employee, the IT department will designate a computer system that must fit the work-related processes.

4. Any user changes and/or termination requests must be submitted via a Help Desk ticket.

5. A member of the Help Desk department will modify, remove or disable access as appropriate.

6. All accounts must have an individual employee or group assigned to be responsible for account management. This may be a combination of the business unit and information technology (IT).

7. Access to GlobeNet´ systems and network resources must be done through the use of individually assigned unique identifiers, known as user-IDs.

8. An authentication token (e.g., password, key fob, biometric) is associated with each user ID, which must be used to authenticate the identity of the person or system requesting access.

9. Automated techniques and controls must be implemented to lock a session and require authentication or re-authentication after a period of inactivity for any system where authentication is required. Information on the screen must be replaced with publicly viewable information (e.g., screen saver, blank screen, clock) during the session lock.

10. Automated techniques and controls must be implemented to terminate a session after specific conditions are met.

11. [Internal and Confidential Information]

12. Passwords used to authenticate a person or process must be treated as confidential and protected appropriately.

13. Passwords must not be stored on paper, or in an electronic file, hand-held device or browser, unless they can be stored securely and the method of storing (e.g., password vault) has been approved by the ISO/designated security representative.

14. *[Internal and Confidential Information]*

15. Information owners are responsible for determining who should have access to protected resources within their jurisdiction, and what those access privileges should be (read, update, etc.).

16. Access privileges will be granted in accordance with the user's job responsibilities and will be limited only to those necessary to accomplish assigned tasks in accordance with GlobeNet missions and business functions (least privilege).

17. Users of privileged accounts must use a separate, non-privileged account when performing normal business transactions.

18. Advance approval for any remote access connection must be granted by GlobeNet. An assessment must be performed and documented to determine the scope and method of access, the technical and business risks involved and the contractual, process and technical controls required for such connection to take place.

19. All remote connections must be made through managed points-of-entry reviewed by the ISO/designated security representative*. [Internal and Confidential Information]*

20. Working from a remote location must be authorized by management and practices which assure the appropriate protection of data in remote environments must be shared with the individual prior to the individual being granted remote access.

4.9. Physical and Environmental Security

1. Information processing and storage facilities must have a defined security perimeter and appropriate security barriers and access controls.

2. All employees and consultants are required to present their identification badge when entering the Company's buildings and offices. Once inside the building, their ID badge must be visibly worn.

3. A periodic risk assessment must be performed for information processing and storage facilities to determine whether existing controls are operating correctly and if additional physical security measures are necessary. These measures must be implemented to mitigate the risks.

4. Information technology equipment must be physically protected from security threats and environmental hazards. Special controls may also be necessary to protect supporting infrastructure and facilities such as electrical supply and cabling infrastructure.

5. All information technology equipment and information media must be secured to prevent compromise of confidentiality, integrity, or availability in accordance with the classification of information contained therein.

6. Visitors to information processing and storage facilities, including maintenance personnel, must be escorted at all times.

4.10. Personnel Security

1. The workforce must receive general security awareness training, to include recognizing and reporting insider threats, within 30 days of hire.

2. Additional training on specific security procedures, if required, must be completed before access is provided to specific GlobeNet sensitive information not covered in the general security training.

3. All security training must be reinforced at least annually and must be tracked by GlobeNet.

4. GlobeNet must require its workforce to abide by the acceptable use of information technology resources rules, described in this Policy, and establish an auditable process for tracking their acknowledge to the requirements herein.

5. All job positions must be evaluated by Cybersecurity Team to determine whether they require access to sensitive information and/or sensitive information technology assets.

6. GlobeNet must conduct workforce suitability evaluations prior hiring, following the Personnel Screening Policy in place. The suitability determination must provide reasonable grounds for the GlobeNet to conclude that an individual will likely be able to perform the required duties and responsibilities of the subject position without undue risk to the GlobeNet.

7. GlobeNet shall establish a process to review information access upon change of job duties or position.

8. Employees are responsible for ensuring all issued property is returned prior to an employee's separation and accounts are disabled and access is removed immediately upon separation.

4.11. Information Classification

To ensure the proper protection of GlobeNet's Information, it is necessary that the information be immediately classified according to the importance and potential impact it represents for the Organization's business. The GlobeNet uses the following categories:

Public - It will be considered as public information that defined by force of law, or duly authorized for external disclosure. In general, this is information available to the public or that is accessible through public consultation, such as press releases, disclosure of events and lectures, advertising materials, among others. The disclosure of this type of information does not cause harm to the Company, to the holders of personal data or to customers, suppliers or other third parties involved with GlobeNet. Public information can only be changed by Collaborators when authorized by the Information Manager.

Internal use - Information for internal use are those that keep matters exclusively relevant to the internal sphere of GlobeNet, being exclusively used by internal Employees or duly authorized third parties and partners. The misuse of this information may cause damage or medium-level institutional impacts to GlobeNet, including documents produced in GlobeNet's daily operations, such as lists of suppliers, sales information, invoices, among others. Information for internal use may only be disclosed to third parties in strictly necessary and previously authorized situations, such as to comply with legal or contractual obligations.

Restricted – Restricted information is information that, due to its nature, must be limited to specific and previously authorized Employees. Such information, if disclosed internally or externally, has the potential to cause serious harm to the holders of personal data or to customers, suppliers or other third parties involved with GlobeNet. In general, this is information related to GlobeNet's business secrets (including budget, new products, strategic projects, customer lists), sensitive personal data of Employees, internal sanctions applied to Employees or judicial or administrative proceedings. Such information must be kept internally and disclosed to other Collaborators or third parties in strictly necessary situations and provided that these individuals are part of the previously authorized group of people.

Highly confidential – Use of highly confidential information is restricted to a certain number of previously authorized Employees and only to senior management positions at GlobeNet, such as President, Vice-Presidents, Directors, and Managers, in order to carry out their activities related to the Company, including long-term business strategies, ongoing critical business negotiations, results of internal audits, among others. The disclosure of this type of information can cause the most serious damage and harm to the holders of personal data or to customers, suppliers or other third parties involved with GlobeNet, such as loss of competitive advantages, image depreciation, loss of business and customers, sanctions administrative and judicial proceedings. Such information must be maintained internally and restricted only to authorized employees.

Based on three principles of security: 1) confidentiality, 2) integrity, and 3) availability each principle, information can be classified as low, moderate, or high impact. Impact levels are defined as limited, serious, and severe or catastrophic.

Categories	Potential Impact	Definitions
Public / Internal use	Low	The potential impact is low if—The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Restricted	Moderate	The potential impact is moderate if—The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
Highly confidential	High	The potential impact is high if—The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

By unifying three principles of security, categories and potential impacts, we obtain Information Asset Classification Matrix:

	Public / Internal Use	Restrict	Highly confidential

	LOW	MODERATE	HIGH
CONFIDENTIALITY Consider impact of unauthorized disclosure.	The unauthorized disclosure of information could be expected to have **limited or no impact** on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious impact** on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe** or **catastrophic impact** on organizational operations, organizational assets, or individuals.
INTEGRITY Consider impact of unauthorized modification or destruction	The unauthorized modification or destruction of information could be expected to have limited or **no impact** on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious impact** on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe** or **catastrophic impact** on organizational operations, organizational assets, or individuals.
AVAILABILITY Consider impact of untimely or unreliable access to information	The disruption of access to or use of information or an Information System could be expected to have limited or **no impact** on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an Information System could be expected to have a **serious impact** on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an Information System could be expected to have a **severe** or **catastrophic impact** on organizational operations, organizational assets, or individuals.

1. The information classification process must include the following:
   a. Identification of information assets;
   b. Classification of information assets; by categories and considering confidentiality, integrity, and availability (“CIA”); and
   c. Determining controls based upon the classification.

2. All information assets must be identified and, when possible, appropriately grouped for a more efficient application of controls of security.

3. An information owner must be determined by a higher level of management. The information owner is responsible for determining the information’s classification, how and by whom the information will be used.

4. An information custodian must be determined. Information custodians are people, units, or organizations responsible for implementing the authorized controls for information assets based on the information owner's requirements and the classification level.

4.12. Systems Security

Systems include but are not limited to servers, platforms, networks, communications, databases and software applications.

1. An individual or group must be assigned responsibility for maintenance and administration of any system deployed on behalf of GlobeNet. A list of assigned individuals or groups must be centrally maintained.
2. Security must be considered at system inception and documented as part of the decision to create or modify a system.
3. All systems must be developed, maintained and decommissioned in accordance with a secure system development lifecycle (SSDLC).
4. Each system must have a set of controls commensurate with the classification of any data that is stored on or passes through the system.
5. All system clocks must synchronize to a centralized reference time source set to UTC (Coordinated Universal Time) which is itself synchronized to at least three synchronized time sources.
6. Environments and test plans must be established to validate the system works as intended prior to deployment in production.
7. Separation of environments (e.g., development, test, quality assurance, production) is required, either logically or physically, including separate environmental identifications (e.g., desktop background, labels).
8. Formal change control procedures for all systems must be developed, implemented and enforced. At a minimum, any change that may affect the production environment and/or production data must be included.

   a. Databases and Software (including in-house or third party developed and commercial off the shelf (COTS):

      i. All software written for or deployed on systems must incorporate secure coding practices, to avoid the occurrence of common coding vulnerabilities and to be resilient to high-risk threats, before being deployed in production.
      ii. Once test data is developed, it must be protected and controlled for the life of the testing in accordance with the classification of the data.
      iii. Production data may be used for testing only if a business case is documented and approved in writing by the information owner and the following controls are applied:

- All security measures, including but not limited to access controls, system configurations and logging requirements for the production data are applied to the test environment and the data is deleted as soon as the testing is completed; or
- sensitive data is masked or overwritten with fictional information.

iv. Where technically feasible, development software and tools must not be maintained on production systems.

v. Where technically feasible, source code used to generate an application or software must not be stored on the production system running that application or software.

vi. Scripts must be removed from production systems, except those required for the operation and maintenance of the system.

vii. Privileged access to production systems by development staff must be restricted.

viii. Migration processes must be documented and implemented to govern the transfer of software from the development environment up through the production environment.

b. Network Systems:

i. Connections between systems must be authorized by the executive management of GlobeNet and protected by the implementation of appropriate controls.

ii. All connections and their configurations must be documented and the documentation must be reviewed by the information owner and the ISO/designated security representative annually, at a minimum, to assure:

- the business case for the connection is still valid and the connection is still required; and
- the security controls in place (filters, rules, access control lists, etc.) are appropriate and functioning correctly.

iii. A network architecture must be maintained that includes, at a minimum, tiered network segmentation between:

- Internet accessible systems and internal systems;
- systems with high security categorizations (e.g., mission critical, systems containing PII) and other systems; and
- user and server segments.

iv. Network management must be performed from a secure, dedicated network.

v. Authentication is required for all users connecting to internal systems.

vi. Network authentication is required for all devices connecting to internal networks.

vii. Firewalls must be implemented to all network segment, especially on critical segments.

viii. Only authorized individuals or business units may capture or monitor network traffic.

ix. A risk assessment must be performed in consultation with the ISO/designated security representative before the initiation of, or significant change to, any network technology or project, including but not limited to wireless technology.

4.13. Operations Security

1. All systems and the physical facilities in which they are stored must have documented operating instructions, management processes and formal incident management procedures related to information security matters which define roles and responsibilities of affected individuals who operate or use them.
2. System configurations must follow approved configuration standards.
3. Advance planning and preparation must be performed to ensure the availability of adequate capacity and resources. System capacity must be monitored on an ongoing basis.
4. Where an Organization provides a server, application or network service to GlobeNet (or vice-versa), operational and management responsibilities must be coordinated by all affected parties.
5. Host based firewalls must be installed and enabled on all workstations to protect from threats and to restrict access to only that which is needed.
6. Controls must be implemented (e.g., anti-virus, software integrity checkers, web filtering) across systems where technically feasible to prevent and detect the introduction of malicious code or other threats.
7. Controls must be implemented to disable automatic execution of content from removable media.
8. Controls must be implemented to limit storage of information to authorized locations.
9. Controls must be in place to allow only approved software to run on a system and prevent execution of all other software.
10. All systems must be maintained at a vendor-supported level to ensure accuracy and integrity.
11. All security patches must be reviewed, evaluated and appropriately applied in a timely manner. This process must be automated, where technically possible.
12. Systems which can no longer be supported or patched to current versions must be removed. In the case of obsolete but essential systems, which cannot be removed or replaced, security compensating controls must be established.
13. Systems and applications must be monitored and analyzed to detect deviation from the access control requirements outlined in this policy and the Security Logging Standard, and record events to provide evidence and to reconstruct lost or damaged data.
14. Audit logs recording and other security-relevant events must be produced, protected and kept Because of the nature of the data contained in this security logs (e.g., passwords, e-mail content).

they can be considered personally identifying information (PII) and must be protected with the controls for a confidentiality and integrity of high.

15. Within the consolidated log infrastructure, logs must be maintained and readily available (online) for a minimum of 90 days. Data stored and maintained through backups and/or other (cold) storage mechanisms must be maintained for a minimum of 1 year. Based on entity requirements, including auditing or legal needs, logs may need to be retained for a longer period of time.

16. Log data must be securely disposed of (at both the system and the infrastructure level) in compliance with the Sanitization/Secure Disposal Standard.

17. Systems that collect logs, whether local or consolidated, must maintain sufficient storage space to meet the minimum requirements for both readily available and retained logs. Storage planning must account for log bursts or increases in storage requirements that could reasonably be expected to result from system issues, including security.

18. A process must be put in place to provide for log preservation requests, such as a legal requirement to prevent the alteration and destruction of particular log records (e.g., how the impacted logs must be marked, stored, and protected).

19. Log integrity for consolidated log infrastructure needs to be preserved, such as storing logs on write-once media or generating message digests for each log file.

20. Access to log management systems must be recorded and must be limited to individuals with a specific need for access to the records. Access to log data must be limited to the specific sets of data appropriate for the business need.

21. Procedures must exist for managing unusual events. Response must be commensurate with system criticality, data sensitivity and regulatory requirements.

22. Monitoring systems must be deployed (e.g., intrusion detection/prevention systems) at strategic locations to monitor inbound, outbound and internal network traffic.

23. Monitoring systems must be configured to alert incident response personnel to indications of compromise or potential compromise.

24. Contingency plans (e.g., business continuity plans, disaster recovery plans, continuity of operations plans) must be established and tested regularly. To know:

    a. An evaluation of the criticality of systems used in information processing (including but not limited to software and operating systems, firewalls, switches, routers and other communication equipment).
    b. Recovery Time Objectives (RTO)/Recovery Point Objectives (RPO) for all critical systems.

25. Backup copies of information, software, and system images must be taken regularly in accordance with the GlobeNet’s defined requirements.

26. Backups and restoration must be tested regularly. Separation of duties must be applied to these functions.

27. Procedures must be established to maintain information security during an adverse event. For those controls that cannot be maintained, compensatory controls must be in place.

4.14. Encryption

1. The need for encryption of information is based on its classification, risk assessment results, and use case.

2. *[Internal and Confidential Information]*

3. Use of outdated, cryptographically broken, proprietary encryption algorithms/hashing functions is prohibited.

4. Electronic information used to authenticate the identity of an individual or process (i.e., PIN, password, passphrase) must be encrypted when stored, transported or transmitted. This does not include the distribution of a one-time use PIN, password, passphrase, token code, etc., provided it is not distributed along with any other authentication information (e.g., user-ID).

5. A system's security plan must include documentation to show appropriate review of encryption methodologies and products. This will demonstrate due diligence in choosing a method or product that has received substantial positive review by reputable third-party analysts.

   a. Encryption is required for data in the following situations:

      i. When electronic personally identifying information (PII) is transmitted (including, but not limited to, e-mail, File Transfer Protocol (FTP), instant messaging, e-fax, Voice Over Internet Protocol (VoIP), etc.).
      ii. When encryption of data in transit is prescribed by law or regulation.
      iii. When connecting to the internal network(s) over a wireless network.
      iv. When remotely accessing a GlobeNet's internal network(s) or devices over a shared (e.g., Internet) or personal (e.g., Bluetooth, infrared) network. This does not apply to remote access over a GlobeNet's managed point to point dedicated connection.
      v. When data is being transmitted with a GlobeNet´s public facing website and/or web services, they are required to utilize Hypertext Transfer Protocol Secure (HTTPS) in lieu of Hypertext Transfer Protocol (HTTP) where technically feasible. Public facing websites must utilize HTTP Strict Transport Security (HSTS), automatically redirecting HTTP requests to HTTPS websites where technically feasible.
      vi. [Internal and Confidential Information]

4.15. Cyber Incident Management

1. GlobeNet must have an incident response plan, consistent standards, to effectively respond to security incidents.

2. The incident response plan must be tested periodically to ensure its effectiveness when used. Those involved must be trained in the execution of the test plan.

3. All observed or suspected information security incidents or weaknesses are to be reported to appropriate management and the ISO/designated security representative as quickly as possible. If a member of the workforce feels that cyber security concerns are not being appropriately addressed, they may confidentially contact the Security Operations Center directly.

4. The Security Operations Center must be notified of any cyber incident which may have a significant or severe impact on operations or security, or which involves digital forensics, to follow proper incident response procedures and guarantee coordination and oversight.

5. Regulatory and supervisory agencies (e.g., CMA) and other legal institutions, when applicable, must be notified observing legal obligations such as those described in cybersecurity and data protection laws.

4.16. Vulnerability Management

1. All systems must be scanned for vulnerabilities before being installed in production and periodically thereafter.

2. All systems are subject to periodic penetration testing.

3. Penetration tests are required periodically for all critical environments/systems.

4. Where the GlobeNet has outsourced a system to another organization or a third party, vulnerability scanning/penetration testing must be coordinated.

5. Scanning/testing and mitigation must be included in third party agreements, where applicable.

6. The output of the scans/penetration tests will be reviewed in a timely manner by the system owner. Copies of the scan report/penetration test must be shared with the ISO/designated security representative for evaluation of risk.

7. Appropriate action, such as patching or updating the system, must be taken to address discovered vulnerabilities. For any discovered vulnerability, a plan of action and milestones must be created, and updated accordingly, to document the planned remedial actions to mitigate vulnerabilities.

8. Any vulnerability scanning/penetration testing must be conducted by individuals who are authorized by the ISO/designated security representative. The CISO must be notified in advance of any such tests. Any other attempts to perform such vulnerability scanning/penetration testing will be deemed an unauthorized access attempt.

9. Anyone authorized to perform vulnerability scanning/penetration testing must have a formal process defined, tested and followed at all times to minimize the possibility of disruption.

5 Compliance

This policy shall take effect upon publication and shall be reviewed annually. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time; compliance with amended policies and standards is expected.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, stakeholders should request an exception through the Chief Information Security Officer's exception process.

6 Annexes

1. Backup Policy Globenet
2. Annex01_BP-02-001-BACKUP POLICY_backup-diagram.vsd.
3. Annex01_BP-02-001-BACKUP POLICY_backup-diagram.vsdx.
4. Annex02_BP_02-001-BACKUP POLICY_Backup-jobs-scope.xlsx.
5. Globenet Retention Policy
6. GlobeNet Global Internal Data Policy
7. Globenet Data Protection Officer Policy
8. Authorized Use Policy
9. Retention Policy
10. Information Security Incident Response Standard

7 Reference

- National Institute of Standards and Technology (NIST) Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.
- Internal Revenue Service Publication 1075: Tax Information Security Guidelines for Federal, State and Local Agencies.