GLOBENET INTERNAL DATA PROTECTION POLICY

Effective date (v.0): June 18, 2021
Update date (v.1): January 12, 2023

Introduction

This policy applies to all employees and contractors with Globenet and its subsidiaries (**"Globenet"** or the **"Company"**). It is intended to provide direction on how to collect, manage and safeguard the Personal Information that Globenet collects, receives, or controls in order to maintain their security, confidentiality, integrity and availability, as well as to comply with applicable laws, regulations and obligations.

Associated Policies

- Globenet Information Security Policy
- Globenet Website Privacy Notice
- Globenet Employee Privacy Notice
- Standard Contractual Clauses

Definitions

1. **Authorized User**: Any employee, temporary worker, consultant, contractor, vendor, agent, volunteer, or other person or entity who is authorized to use Information Assets and/or to access Information related to Globenet's business under the terms and conditions of this policy.

2. **Company Data**: A Company Record in electronic format that is classified as Confidential (which includes Personal Information).

3. **Company Record**: information recorded in any format (electronic or hard copy) that a Company employee creates, receives, or distributes or the Company otherwise controls and relates to the Company or its business.

4. **Contract**: a generic term used to refer to any written document that evidences a binding commitment by the Company to purchase goods or services from a third-party or vendor, or by a customer to purchase goods or services from the Company.

5. **Information Security**: the physical, administrative, and technical safeguards developed and implemented by the Company to protect the security, confidentiality, accuracy, integrity of, and access to, Company Data, including Personal Information.

6. **Information Asset**: Any and all digital, electronic, or telecommunication resources that are used in Globenet's offices, during business travel, or

otherwise provided by Globenet for the purpose of conducting business on behalf of Globenet. Information Assets include, but are not limited to, physical resources such as telephones, cameras, cell phones, tablets, computers, laptops, fax machines, printers, scanners, copiers, removable-storage devices (e.g., USBs, CDs, DVDs, removable hard drives) and non-physical resources such as company intranets, applications on Globenet's network, cloud-based networks and software, internet and Globenet network access and connectivity, phone systems, email, instant messaging, accounts, voicemail, collaboration tools and Globenet social-media sites.

7. **Personal Information**: information related to an identified or identifiable natural person, including data collected from consumers, customers, Globenet employees, suppliers, vendors, applicants, or others that identifies or can be used to identify, an individual. Personal Information can be in either electronic or hard copy format.

8. **Privacy**: the appropriate use of Personal Information as defined by law.

9. **Privacy Policy**: a written declaration of the Company's Privacy practices, e.g., what types of Personal Information the Company will collect, and how it will use, store, protect and dispose of the Personal Information.

a. You must collect Personal Information only by lawful means, such as for legitimate business objectives or by the individual's consent. For purposes of the policy, collection includes Personal Information collected by Globenet employees and by third parties on the Company's behalf.

b. You must protect Personal Information against unauthorized disclosure, modification, compromise, or destruction.

c. You must collect Personal Information only as reasonably necessary to accomplish Globenet's business objectives or as necessary to validate the identity of the individual from whom the Personal Information is collected.

d. You must manage Personal Information in a manner consistent with applicable Privacy Policy and in accordance with Company policies and procedures. Refer to the Website Privacy Policy, Information Security Policy, and related procedures for guidance.

e. You must take reasonable steps to assure that Personal Information is accurate, complete, up to date and not corrupted or inadvertently changed.

f. You must securely dispose of Company Records containing Personal Information, once they are no longer subject to retention under the applicable Business Hold

List or Legal Hold Notice, in accordance with company retention policies and related procedures, including by shredding, permanently erasing, or otherwise modifying the Personal Information to make it unreadable or undecipherable.

Encryption

a. If you are sharing or transmitting Information outside of Globenet, you must take measures to protect the confidentiality and security of Company Data, using Globenet approved encryption and other tools for sending or sharing Company Data or Personal Information outside of Globenet's network. Contact Globenet's Data Protection Officer ("DPO") at dpo@globenet.net for assistance with transmission of Personal Information outside of Globenet's systems.

b. You must encrypt the following types of Personal Information when emailed or transmitted electronically outside the Globenet family of companies: social security number (or national equivalent), driver's license number, passport number, bank account number, credit card number or debit card number.

c. You must encrypt the types of Personal Information described above when stored on portable devices or media. You may only store these types of Personal Information on Company-issued portable devices or media

Accessing and Disclosing Company Data

a. Only Authorized Users may access Personal Information and/or Company Data.

b. Information, including Information about Globenet's activities, business plans, products, associates, and customers, must not be disclosed outside of Globenet without approval from management who has ownership responsibility or without secured appropriate protections for that Information.

c. If you become aware of any unauthorized use of Company Data, any weaknesses in Globenet computer security, or any other security related issue, contact Globenet's DPO at dpo@globenet.net immediately. As an Authorized User, you are responsible for complying with all applicable policies in your use of Information and Information Assets. You are responsible for the security of Information and Information Assets under your control.

d. You may access Personal Information or transfer it to other Globenet employees only under the following circumstances:
    i. When necessary to perform your or the other Globenet employee's job responsibilities

ii. When necessary to comply with a Company policy or procedure or to prevent the violation of a Company policy
iii. When authorized to do so in connection with an internal investigation of an actual or suspected compliance violation or illegal activity
iv. When required by applicable law or legal process

e. You may disclose or transfer Personal Information to third parties only under the following circumstances:
    i. When necessary to comply with Globenet's contractual obligations with third parties
    ii. When necessary for a third-party to perform services for the Company
    iii. When necessary to prevent actual or potential physical harm or financial loss
    iv. When authorized to do so in connection with an internal or external investigation of an actual or suspected compliance violation or illegal activity
    v. When required by applicable law or legal process

Contract Requirements

a. Contracts with third parties who have access to Personal Information must contain provisions requiring the third party to protect the Personal Information against unauthorized access, use and disclosure. Contracts with third parties outside of the scope of Brazil's LGPD must adhere to the Standard Contractual Clauses. Globenet's DPO is responsible for developing and approving these Contract provisions and may approve modified Contract provisions on a case by case basis.

b. Before giving a third party access to Personal Information, you must confirm that they are contractually obligated to protect the Personal Information in accordance with Contract provisions approved by Globenet's DPO. If you are unsure if the third party is contractually obligated to do so, contact dpo@globenet.net.

c. If you are a relationship manager for a third party who has access to Personal Information, you must:
    i. Ensure that the third party is contractually obligated to protect the Personal Information in accordance with Contract provisions approved by Globenet's DPO; and

    ii. Confirm that the third party's practices comply with its contractual obligations to protect the Personal Information.

Information Asset Management

a. Globenet hardware must be protected from actions that could jeopardize the confidentiality, integrity, or availability of Information and automated

systems. You should pay particular attention to your surroundings, making every effort to protect Globenet Information and Information Assets from unauthorized access. At all times and especially when in public areas, Authorized Users must protect Sensitive Information from "shoulder surfing" by positioning workstation or laptop screens away from visibility.

b. Globenet hardware is provided for conducting Globenet business and management-approved activities. When no longer needed, hardware must be returned timely.

c. Only Globenet owned or leased hardware may be used on the Globenet network. Non Globenet owned or leased hardware is permitted to connect to the Globenet network only through approved and designated gateways.

Clear Desk and Clear Screen

a. Authorized Users are expected to protect Sensitive Information that they create, access and/or use, including:
    i. Clear Desk: Authorized Users are required to remove Sensitive Information from their open work area anytime their work area cannot be monitored during the workday. Authorized Users are required to remove and secure Sensitive Information from their open work area before leaving at the end of the day.

    ii. Clear Screen: Authorized Users are required to lock their screens in any situation where they are away from their computer, including for meetings, restroom breaks, and lunch.

    iii. End of Day: Before leaving at the end of the day, Authorized users are required to power down the computer.

    iv. Offices: If an office door can be locked, the removal of Sensitive Information from the work area is not required if the office door is shut and locked.

    v. File Cabinets: Cabinets containing Sensitive Information must be locked at all times when not in use.

    vi. Printers: Sensitive Information must not be left unattended at printers.

b. Unattended work areas must be clear of Sensitive Information in any form.

Network and Communications Security

a. Connections to non-Globenet computers and networks must be implemented in a controlled and secure manner to ensure the confidentiality, integrity, availability, and authenticity of Information transmitted between Globenet computer systems and outside networks and

computers. Implementers and administrators of the network and network-perimeter security technologies are responsible for adhering to key control standards.

b. Remote access to Information Assets, wherever they reside, must be approved through multi-factor authentication and must be approved by your manager.
c. Only Globenet approved applications may be used for business purposes. You may not use personal email or storage (e.g., Gmail, Hotmail, iCloud, Google Drive, DropBox, OneDrive) for business purposes.
d. Only approved licensed software may be loaded on Globenet workstations, laptops, and servers.

Anti-Virus and Malware Protection

a. Anti-Virus and Malware Protection software must be used, and must not be disabled, to protect Information from virus infection.
b. You may not download, install, or run programs designed to test the security of Globenet Information Assets or reveal or exploit weaknesses in security unless you are authorized to do so.

Responding to Computer and Information Security Breaches

a. If you know or suspect that a computer or Information Security breach has occurred, you must contact Globenet's DPO at dpo@globenet.net or +55 21 3475 3320 (Brazil) / +1 561 544 6579 (USA) / +57 1 650 5198 (Colombia) / +1-441-297-3711 (Bermuda) / +58.212-740-4160 Venezuela) immediately. Refer to the Information Security Policy for additional guidance.

b. Examples of computer and Information Security breaches include:
    i. Suspected or actual loss, theft or compromise of electronic equipment containing Company Records. Electronic equipment includes computers, cell phones, portable devices and storage media. This applies to any equipment that contains Company Records, whether the equipment is Company-issued, or owned by a Company employee or vendor.
    ii. Suspected or actual loss or theft of hard copy documents containing Company Records.
    iii. Suspected or actual unauthorized access to Company Data