Workstation Policy

D

O

L

P

H

I

N

I

N

C

J

u

l

y

2

0

2

Contents

1

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC6.8

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document

1 Purpose and Scope

a. This policy defines best practices to reduce the risk of data loss/exposure through workstations.

b. This policy applies to all employees and contractors. Workstation is defined as the collection of all company-owned and personal devices containing company data.

2 Policy

a. Workstation devices must meet the following criteria:

   i. Operating system must be no more than one generation older than current

   ii. Device must be encrypted at rest

   iii. Device must be locked when not in use or when employee leaves the workstation

   iv. Workstations must be used for authorized business purposes only

   v. Loss or destruction of devices should be reported immediately

   vi. Laptops and desktop devices should run the latest version of antivirus software that has been approved by IT

b. Desktop & laptop devices

   i. Employees will be issued a desktop, laptop, or both by the company, based on their job duties. Contractors will provide their own laptops.

   ii. Desktops and laptops must operate on macOS or Windows.

c. Mobile devices

   i. Mobile devices must be operated as defined in the Removable Media Policy, Cloud Storage, and Bring Your Own Device Policy.

   ii. Mobile devices must operate on iOS or Android.

   iii. Company data may only be accessed on mobile devices with Slack and Gmail.

d. Removable media

   i. Removable media must be operated as defined in the Removable Media Policy, Cloud Storage, and Bring Your Own Device Policy.

   ii. Removable media is permitted on approved devices as long as it does not conflict with other policies.

Vendor Management Policy

Contents

D

O

L

P

H

I

N

I

N

C

J

u

l

y

2

0

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC9.2

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document

1 Purpose and Scope

a. This policy defines the rules for relationships with the organization's Information Technology (IT) vendors and partners.

b. This policy applies to all IT vendors and partners who have the ability to impact the confidentiality, integrity, and availability of the organization's technology and sensitive information, or who are within the scope of the organization's information security program.

c. This policy applies to all employees and contractors that are responsible for the management and oversight of IT vendors and partners of the organization.

2 Background

a. The overall security of the organization is highly dependent on the security of its contractual relationships with its IT suppliers and partners. This policy defines requirements for effective management and oversight of such suppliers and partners from an information security perspective. The policy prescribes minimum standards a vendor must meet from an information security standpoint, including security clauses, risk assessments, service level agreements, and incident management.

3 References

a. Information Security Policy

b. Security Incident Response Policy

4 Policy

a. IT vendors are prohibited from accessing the organization's information security assets until a contract containing security controls is agreed to and signed by the appropriate parties.

b. All IT vendors must comply with the security policies defined and derived from the Information Security Policy (reference (a)).

c. All security incidents by IT vendors or partners must be documented in accordance with the organization's Security Incident Response Policy (reference (b)) and immediately forwarded to the Information Security Manager (ISM).

d. The organization must adhere to the terms of all Service Level Agreements (SLAs) entered into with IT vendors. As terms are updated, and as new

ones are entered into, the organization must implement any changes or controls needed to ensure it remains in compliance.

e. Before entering into a contract and gaining access to the parent organization's information systems, IT vendors must undergo a risk assessment.
    i. Security risks related to IT vendors and partners must be identified during the risk assessment process.
    ii. The risk assessment must identify risks related to information and communication technology, as well as risks related to IT vendor supply chains, to include sub-suppliers.
f. IT vendors and partners must ensure that organizational records are protected, safeguarded, and disposed of securely. The organization strictly adheres to all applicable legal, regulatory and contractual requirements regarding the collection, processing, and transmission of sensitive data such as Personally-Identifiable Information (PII).
g. The organization may choose to audit IT vendors and partners to ensure compliance with applicable security policies, as well as legal, regulatory and contractual obligations.

Vendor Management Policy

Contents

D

O

L

P

H

I

N

I

N

C

J

u

l

y

2

0

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC9.2

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document

1 Purpose and Scope

a. This policy defines the rules for relationships with the organization's Information Technology (IT) vendors and partners.

b. This policy applies to all IT vendors and partners who have the ability to impact the confidentiality, integrity, and availability of the organization's technology and sensitive information, or who are within the scope of the organization's information security program.

c. This policy applies to all employees and contractors that are responsible for the management and oversight of IT vendors and partners of the organization.

2 Background

a. The overall security of the organization is highly dependent on the security of its contractual relationships with its IT suppliers and partners. This policy defines requirements for effective management and oversight of such suppliers and partners from an information security perspective. The policy prescribes minimum standards a vendor must meet from an information security standpoint, including security clauses, risk assessments, service level agreements, and incident management.

3 References

a. Information Security Policy

b. Security Incident Response Policy

4 Policy

a. IT vendors are prohibited from accessing the organization's information security assets until a contract containing security controls is agreed to and signed by the appropriate parties.

b. All IT vendors must comply with the security policies defined and derived from the Information Security Policy (reference (a)).

c. All security incidents by IT vendors or partners must be documented in accordance with the organization's Security Incident Response Policy (reference (b)) and immediately forwarded to the Information Security Manager (ISM).

d. The organization must adhere to the terms of all Service Level Agreements (SLAs) entered into with IT vendors. As terms are updated, and as new

ones are entered into, the organization must implement any changes or controls needed to ensure it remains in compliance.

e. Before entering into a contract and gaining access to the parent organization's information systems, IT vendors must undergo a risk assessment.
    i. Security risks related to IT vendors and partners must be identified during the risk assessment process.
    ii. The risk assessment must identify risks related to information and communication technology, as well as risks related to IT vendor supply chains, to include sub-suppliers.
f. IT vendors and partners must ensure that organizational records are protected, safeguarded, and disposed of securely. The organization strictly adheres to all applicable legal, regulatory and contractual requirements regarding the collection, processing, and transmission of sensitive data such as Personally-Identifiable Information (PII).
g. The organization may choose to audit IT vendors and partners to ensure compliance with applicable security policies, as well as legal, regulatory and contractual obligations.

Security Incident Response Policy

DOLPHI

N INC

July 2021

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied TSC
	CC7.3, CC7.4, CC7.5

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document

Security Incident Response Policy

1 Purpose and Scope

a. This security incident response policy is intended to establish controls to ensure detection of security vulnerabilities and incidents, as well as quick reaction and response to security breaches.

b. This document also provides implementing instructions for security in- cident response, to include definitions, procedures, responsibilities, and performance measures (metrics and reporting mechanisms).

c. This policy applies to all users of information systems within the orga- nization. This typically includes employees and contractors, as well as any external parties that come into contact with systems and information controlled by the organization (hereinafter referred to as "users"). This policy must be made readily available to all users.

2 Background

a. A key objective of the organization's Information Security Program is to focus on detecting information security weaknesses and vulnerabilities so that incidents and breaches can be prevented wherever possible. The organization is committed to protecting its employees, customers, and partners from illegal or damaging actions taken by others, either knowingly or unknowingly. Despite this, incidents and data breaches are likely to happen; when they do, the organization is committed to rapidly responding to them, which may include identifying, containing, investigating, resolving
, and communicating information related to the breach.

b. This policy requires that all users report any perceived or actual information security vulnerability or incident as soon as possible using the contact mechanisms prescribed in this document. In addition, the organization must employ automated scanning and reporting mechanisms that can be used to identify possible information security vulnerabilities and incidents. If a vulnerability is identified, it must be resolved within a set period of time based on its severity. If an incident is identified, it must be investigated within a set period of time based on its severity. If an incident is confirmed as a breach, a set procedure must be followed to contain, investigate, resolve, and communicate information to employees, customers, partners and other stakeholders.

c. Within this document, the following definitions apply:

   i. *Information Security Vulnerability:* a vulnerability in an information system, information system security procedures, or administrative controls that could be exploited to gain unauthorized access to infor- mation or to disrupt critical processing.

   ii. *Information Security Incident:* a suspected, attempted, successful, or

imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of information; interference with information technology operations; or significant violation of information security policy.

3 Policy

a. All users must report any system vulnerability , incident, or event pointing to a possible incident to the Information Security Manager (ISM) as quickly as possible but no later than 24 hours. Incidents must be reported by sending an email message to with details of the incident.

b. Users must be trained on the procedures for reporting information security incidents or discovered vulnerabilities, and their responsibilities to report such incidents. Failure to report information security incidents shall be considered to be a security violation and will be reported to the Human Resources (HR) Manager for disciplinary action.

c. Information and artifacts associated with security incidents (including but not limited to files, logs, and screen captures) must be preserved in the event that they need to be used as evidence of a crime.

d. All information security incidents must be responded to through the incident management procedures defined below.

e. In order to appropriately plan and prepare for incidents, the organization must review incident response procedures at least once per year for currency, and update as required.

f. The incident response procedure must be tested on at least twice per year

g. The incident response logs must be reviewed once per month to assess response effectiveness.

4 Procedure For Establishing Incident Response System

a. Define on-call schedule and assign an Information Security Manager (ISM) responsible for managing incident response procedure during each avail- ability window.

b. Define notification channel to alert the on-call ISM of a potential security incident. Establish company resource that includes up to date contact information for on-call ISM.

c. Assign management sponsors from the Engineering, Legal, HR, Marketing, and C-Suite teams.

d. Distribute Procedure For Execute Incident Response to all staff and ensure up-to-date versions are accessible in a dedicated company resource.

e. Require all staff to complete training for Procedure For Executing Incident Response at least twice per year.

5 Procedure For Executing Incident Response

a. When an information security incident is identified or detected, users must notify their immediate manager within 24 hours. The manager must immediately notify the ISM on call for proper response. The following information must be included as part of the notification:

   i. Description of the incident

   ii. Date, time, and location of the incident

   iii. Person who discovered the incident

   iv. How the incident was discovered

   v. Known evidence of the incident

   vi. Affected system(s)

b. Within 48 hours of the incident being reported, the ISM shall conduct a preliminary investigation and risk assessment to review and confirm the details of the incident. If the incident is confirmed, the ISM must assess the impact to the organization and assign a severity level, which will determine the level of remediation effort required:

   i. High: the incident is potentially catastrophic to the organization and/or disrupts the organization's day-to-day operations; a violation of legal, regulatory or contractual requirements is likely.

   ii. Medium: the incident will cause harm to one or more business units within the organization and/or will cause delays to a business unit's activities.

   iii. Low: the incident is a clear violation of organizational security policy, but will not substantively impact the business.

c. The ISM, in consultation with management sponsors, shall determine appropriate incident response activities in order to contain and resolve incidents.

d. The ISM must take all necessary steps to preserve forensic evidence (e.g. log information, files, images) for further investigation to determine if any malicious activity has taken place. All such information must be preserved and provided to law enforcement if the incident is determined to be malicious.

e. If the incident is deemed as High or Medium, the ISM must work with the VP Brand/Creative, General Counsel, and HR Manager to create and execute a communications plan that communicates the incident to users, the public, and others affected.

f. The ISM must take all necessary steps to resolve the incident and recover information systems, data, and connectivity. All technical steps taken during an incident must be documented in the organization's incident log, and must contain the following:

   i. Description of the incident

   ii. Incident severity level

   iii. Root cause (e.g. source address, website malware, vulnerability)

   iv. Evidence

   v. Mitigations applied (e.g. patch, re-image)

   vi. Status (open, closed, archived)

   vii. Disclosures (parties to which the details of this incident were disclosed to, such as customers, vendors, law enforcement, etc.)

g. After an incident has been resolved, the ISM must conduct a post mortem that includes root cause analysis and documentation any lessons learned.

h. Depending on the severity of the incident, the Chief Executive Officer (CEO) may elect to contact external authorities, including but not limited to law enforcement, private investigation firms, and government organizations as part of the response to the incident.

i. The ISM must notify all users of the incident, conduct additional training if necessary, and present any lessons learned to prevent future occurrences. Where necessary, the HR Manager must take disciplinary action if a user's activity is deemed as malicious.

Security Architecture Narrative

D

O

L

P

H

I

N

I

N

C

J

u

l

y

2

0

2

1

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC6.6, CC6.7, CC7.1, CC7.2

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document

1 Security Architecture Narrative

Here we narrate why our org satisfies the control keys listed in the YML block

2 DOLPHIN INC Product Architecture

Describe product architecture here, emphasizing security implications

3 DOLPHIN INC Infrastructure

3.1 Product Infrastructure

Describe product infrastructure, emphasizing security measures

3.1.1 Authorized Personnel

- **AWS root account** access is granted only to the CTO and CEO
- **AWS IAM** access is granted to to a limited group of **Operators**
- **DOLPHIN INC SSH** access is granted to a limited group of **Operators**
- **DOLPHIN INC DB** access is granted to a limited group of **Data Operators**

3.2 IT Infrastructure

DOLPHIN INC uses the following cloud services for its internal infrastructure:

- List cloud services

Access to these cloud services is limited according to the role of the DOLPHIN INC employee and is reviewed quarterly as well as via regular onboarding/offboarding tasks for new and departing employees.

4 DOLPHIN INC Workstations

DOLPHIN INC workstations are hardened against logical and physical attack by the following measures:

- operating system must be within one generation of current
- full-disk encryption
- onboard antivirus/antimalware software
- OS and AV automatically updated

Workstation compliance with these measures is evaluated on a quarterly basis.

4.1 Remote Access

Many DOLPHIN INC employees work remotely on a regular basis and connect to production and internal IT systems via the same methods as those employees

connecting from the DOLPHIN INC physical office, i.e., direct encrypted access to cloud services. It is the employee's responsibility to ensure that only authorized personnel use DOLPHIN INC resources and access DOLPHIN INC systems.

5 Access Review

Access to DOLPHIN INC infrastructure, both internal and product, is reviewed quarterly and inactive users are removed. Any anomalies are reported to the security team for further investigation. When employees start or depart, an onboarding/offboarding procedure is followed to provision or deprovision appropriate account access.

6 Penetration Testing

DOLPHIN INC commissions an external penetration test on an annual basis. All findings are immediately reviewed and addressed to the satisfaction of the CTO/CEO.

7 DOLPHIN INC Physical Security

DOLPHIN INC has one physical location, in San Francisco, CA. Key issuance is tracked by the Office Physical Security Policy Ledger. Office keys are additionally held by the lessor, property management, and custodial staff. These keys are not tracked by the Office Physical Security Policy Ledger. DOLPHIN INC managers regularly review physical access privileges.

DOLPHIN INC infrastructure is located within AWS. DOLPHIN INC does not have physical access to AWS infrastructure.

8 Risk Assessment

DOLPHIN INC updates its Cyber Risk Assessment on an annual basis in order to keep pace with the evolving threat landscape. The following is an inventory of adversarial and non-adversarial threats assessed to be of importance to DOLPHIN INC.

8.1 Adversarial Threats

The following represents the inventory of adversarial threats:

Threat	Source	Vector	Target	Likelihood	Severity

8.2 Non-Adversarial Threats

The following represents the inventory of non-adversarial threats:

Threat	Vector	Target	Likelihood	Severity

9 References

9.1 Narratives

Products and Services Narrative System Architecture Narrative

9.2 Policies

Encryption Policy Log Management Policy Office Security Policy Remote Access Policy Security Incident Response Policy Workstation Policy

9.3 Procedures

Apply OS Patches Review & Clear Low-Priority Alerts Review Access Review Devices & Workstations

Software Development Lifecycle Policy

DOLPHI

N INC

July 2021

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC8.1

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document

Software Development Lifecycle Policy

1 Purpose and Scope

a. The purpose of this policy is to define requirements for establishing and maintaining baseline protection standards for company software, network devices, servers, and desktops.

b. This policy applies to all users performing software development, system administration, and management of these activities within the organization. This typically includes employees and contractors, as well as any relevant external parties involved in these activities (hereinafter referred to as “users”). This policy must be made readily available to all users.

c. This policy also applies to enterprise-wide systems and applications developed by the organization or on behalf of the organization for production implementation.

2 Background

a. The intent of this policy is to ensure a well-defined, secure and consistent process for managing the entire lifecycle of software and information systems, from initial requirements analysis until system decommission. The policy defines the procedure, roles, and responsibilities, for each stage of the software development lifecycle.

b. Within this policy, the software development lifecycle consists of requirements analysis, architecture and design, development, testing, deployment/implementation, operations/maintenance, and decommission. These processes may be followed in any form; in a waterfall model, it may be appropriate to follow the process linearly, while in an agile development model, the process can be repeated in an iterative fashion.

3 References

a. Risk Assessment Policy

4 Policy

a. The organization’s Software Development Life Cycle (SDLC) includes the following phases:

   i. Requirements Analysis

   ii. Architecture and Design

   iii. Testing

   iv. Deployment/Implementation

v. Operations/Maintenance

vi. Decommission

b. During all phases of the SDLC where a system is not in production, the system must not have live data sets that contain information identifying actual people or corporate entities, actual financial data such as account numbers, security codes, routing information, or any other financially identifying data. Information that would be considered sensitive must never be used outside of production environments.

c. The following activities must be completed and/or considered during the requirements analysis phase:

i. Analyze business requirements.

ii. Perform a risk assessment. More information on risk assessments is discussed in the Risk Assessment Policy (reference (a)).

iii. Discuss aspects of security (e.g., confidentiality, integrity, availability) and how they might apply to this requirement.

iv. Review regulatory requirements and the organization's policies, standards, procedures and guidelines.

v. Review future business goals.

vi. Review current business and information technology operations.

vii. Incorporate program management items, including:

1. Analysis of current system users/customers.

2. Understand customer-partner interface requirements (e.g., business-level, network).

3. Discuss project timeframe.

viii. Develop and prioritize security solution requirements.

ix. Assess cost and budget constraints for security solutions, including development and operations.

x. Approve security requirements and budget.

xi. Make "buy vs. build" decisions for security services based on the information above.

d. The following must be completed/considered during the architecture and design phase:

i. Educate development teams on how to create a secure system.

ii. Develop and/or refine infrastructure security architecture.

iii. List technical and non-technical security controls.

iv. Perform architecture walkthrough.

v. Create a system-level security design.

vi. Create high-level non-technical and integrated technical security designs.

vii. Perform a cost/benefit analysis for design components.

viii. Document the detailed technical security design.

ix. Perform a design review, which must include, at a minimum, technical reviews of application and infrastructure, as well as a review of high- level processes.

x. Describe detailed security processes and procedures, including: segregation of duties and segregation of development, testing and production environments.

xi. Design initial end-user training and awareness programs.

xii. Design a general security test plan.

xiii. Update the organization's policies, standards, and procedures, if appropriate.

xiv. Assess and document how to mitigate residual application and infrastructure vulnerabilities.

xv. Design and establish separate development and test environments.

e. The following must be completed and/or considered during the development phase:

i. Set up a secure development environment (e.g., servers, storage).

ii. Train infrastructure teams on installation and configuration of appli- cable software, if required.

iii. Develop code for application-level security components.

iv. Install, configure and integrate the test infrastructure.

v. Set up security-related vulnerability tracking processes.

vi. Develop a detailed security test plan for current and future versions (i.e., regression testing).

vii. Conduct unit testing and integration testing.

f. The following must be completed and/or considered during the testing phase:

i. Perform a code and configuration review through both static and dynamic analysis of code to identify vulnerabilities.

ii. Test configuration procedures.

iii. Perform system tests.

iv. Conduct performance and load tests with security controls enabled.

v. Perform usability testing of application security controls.

vi. Conduct independent vulnerability assessments of the system, includ- ing the infrastructure and application.

g. The following must be completed and/or considered during the deployment phase:

i. Conduct pilot deployment of the infrastructure, application and other relevant components.

ii. Conduct transition between pilot and full-scale deployment.

iii. Perform integrity checking on system files to ensure authenticity.

iv. Deploy training and awareness programs to train administrative per- sonnel and users in the system's security functions.

v. Require participation of at least two developers in order to conduct full-scale deployment to the production environment.

h. The following must be completed and/or considered during the opera- tions/maintenance phase:

i. Several security tasks and activities must be routinely performed to operate and administer the system, including but not limited to:

1. Administering users and access.
2. Tuning performance.
3. Performing backups according to requirements defined in the System Availability Policy
4. Performing system maintenance (i.e., testing and applying secu- rity updates and patches).
5. Conducting training and awareness.
6. Conducting periodic system vulnerability assessments.
7. Conducting annual risk assessments.

ii. Operational systems must:

1. Be reviewed to ensure that the security controls, both automated and manual, are functioning correctly and effectively.
2. Have logs that are periodically reviewed to evaluate the security of the system and validate audit controls.
3. Implement ongoing monitoring of systems and users to ensure detection of security violations and unauthorized changes.

4. Validate the effectiveness of the implemented security controls through security training as required by the Procedure For Executing Incident Response.
5. Have a software application and/or hardware patching process that is performed regularly in order to eliminate software bug and security problems being introduced into the organization's technology environment. Patches and updates must be applied within ninety (90) days of release to provide for adequate testing and propagation of software updates. Emergency, critical, break- fix, and zero-day vulnerability patch releases must be applied as quickly as possible.

i. The following must be completed and/or considered during the decommission phase:
    i. Conduct unit testing and integration testing on the system after component removal.
    ii. Conduct operational transition for component removal/replacement.
    iii. Determine data retention requirements for application software and systems data.
    iv. Document the detailed technical security design.
    v. Update the organization's policies, standards and procedures, if appropriate.
    vi. Assess and document how to mitigate residual application and infrastructure vulnerabilities.

System Change Policy

D

O

L

P

H

I

N

I

N

C

J

u

l

y

2

0

Contents

Software Development Lifecycle Policy

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC8.1, CC3.4

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document

1 Purpose and Scope

a. This information security policy defines how changes to information systems are planned and implemented

b. This policy applies to the entire information security program at the organization (i.e. to all information and communications technology, as well as related documentation).

c. All employees, contractors, part-time and temporary workers, service providers, and those employed by others to perform work for the organization, or who have been granted to the organization's information and communications technology, must comply with this policy.

2 Background

a. This policy defines specific requirements to ensure that changes to systems and applications are properly planned, evaluated, reviewed, approved, communicated, implemented, documented, and reviewed, thereby ensuring the greatest probability of success. Where changes are not successful, this document provides mechanisms for conducting post-implementation review such that future mistakes and errors can be prevented.

3 Policy

a. Any changes to the security architecture or customer data handling of a system must be formally requested in writing to the organization's Information Security Manager (ISM), and approved by the ISM and the Chief Information Officer (CIO).

b. All change requests must be documented.

c. All change requests must be prioritized in terms of benefits, urgency, effort required, and potential impacts to the organization's operations.

d. All implemented changes must be communicated to relevant users.

e. Change management must be conducted according to the following procedure:

    i. *Planning*: plan the change, including the implementation design, scheduling, and implementation of a communications plan, testing plan, and roll-back plan.

    ii. *Evaluation*: evaluate the change, including priority level of the service and risk that the proposed change introduces to the system; determine the change type and the specific step-by-step process to implement the change.

iii. *Review*: review the change plan amongst the CIO, ISM, Engineering Lead, and, if applicable, Business Unit Manager.

iv. *Approval*: the CIO must approve the change plan.

v. *Communication*: communicate the change to all users of the system.

vi. *Implementation*: test and implement the change.

vii. *Documentation*: record the change and any post-implementation issues.

viii. *Post-change review*: conduct a post-implementation review to determine how the change is impacting the organization, either positively or negatively. Discuss and document any lessons learned.

System Architecture Narrative

DOLPHIN INC July 2020

Contents

2 1

Table 1: Document history

Date	Comment
Jun 1 2018	Initial document

1 System Architecture Narrative

Here we narrate why our org satisfies the control keys listed in the YML block

2 Template Coming Soon

Remote Access Policy

DOLPHIN INC July 2020

Contents

2 1

Table 1: Control satisfaction

Standard	Controls Satisfied TSC
CC6.1, CC6.2, CC6.7	

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document

1 Purpose and Scope

a. The purpose of this policy is to define requirements for connecting to the organization's systems and networks from remote hosts, including personally-owned devices, in order to minimize data loss/exposure.

b. This policy applies to all users of information systems within the orga- nization. This typically includes employees and contractors, as well as any external parties that come into contact with systems and information controlled by the organization (hereinafter referred to as "users"). This policy must be made readily accessible to all users.

2 Background

a. The intent of this policy is to minimize the organization's exposure to damages which may result from the unauthorized remote use of resources, including but not limited to: the loss of sensitive, company confidential data and intellectual property; damage to the organization's public image; damage to the organization's internal systems; and fines and/or other financial liabilities incurred as a result of such losses.

b. Within this policy, the following definitions apply:

   i. *Mobile computing equipment:* includes portable computers, mobile phones, smart phones, memory cards and other mobile equipment used for storage, processing and transfer of data.

   ii. *Remote host:* is defined as an information system, node or network that is not under direct control of the organization.

   iii. *Telework:* the act of using mobile computing equipment and remote hosts to perform work outside the organization's physical premises. Teleworking does not include the use of mobile phones.

3 Policy

a. Security Requirements for Remote Hosts and Mobile Computing Equipment

   i. Caution must be exercised when mobile computing equipment is placed or used in uncontrolled spaces such as vehicles, public spaces, hotel rooms, meeting places, conference centers, and other unprotected areas outside the organization's premises.

   ii. When using remote hosts and mobile computing equipment, users must take care that information on the device (e.g. displayed on the screen) cannot be read by unauthorized persons if the device is being used to connect to the organization's systems or work with the organization's data.

iii. Remote hosts must be updated and patched for the latest security updates on at least a monthly basis.

iv. Remote hosts must have endpoint protection software (e.g. malware scanner) installed and updated at all times.

v. Persons using mobile computing equipment off-premises are responsible for regular backups of organizational data that resides on the the device.

vi. Access to the organization's systems must be done through an encrypted and authenticated VPN connection with multi-factor authentication enabled. All users requiring remote access must be provisioned with VPN credentials from the organization's information technology team. VPN keys must be rotated at least twice per year. Revocation of VPN keys must be included in the Offboarding Policy.

vii. Information stored on mobile computing equipment must be encrypted using hard drive full disk encryption.

b. Security Requirements for Telework

i. Employees must be specifically authorized for telework in writing from their hiring manager .

ii. Only device's assigned owner is permitted to use remote nodes and mobile computing equipment. Unauthorized users (such as others living or working at the location where telework is performed) are not permitted to use such devices.

iii. Devices must be authorized using certificates

iv. Users performing telework are responsible for the appropriate configuration of the local network used for connecting to the Internet at their telework location.

v. Users performing telework must protect the organization's intellectual property rights, either for software or other materials that are present on remote nodes and mobile computing equipment.

Password Policy

Contents

DOLPHIN

I y

N 2

C 0

J 2

u 1

l

Table 1: Control satisfaction

Standard	Controls
Satisfied	TSC CC9.9

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document

1 Purpose and Scope

a. The Password Policy describes the procedure to select and securely manage passwords.

b. This policy applies to all employees, contractors, and any other personnel who have an account on any system that resides at any company facility or has access to the company network.

2 Policy

a. Rotation requirements

i. All system-level passwords should be rotated on at least a quarterly basis. All user-level passwords should be rotated at least every six months.

ii. If a credential is suspected of being compromised, the password in question should be rotated immediately and the Engineering/Security team should be notified.

b. Password protection

i. All passwords are treated as confidential information and should not be shared with anyone. If you receive a request to share a password, deny the request and contact the system owner for assistance in provisioning an individual user account.

ii. Do not write down passwords, store them in emails, electronic notes, or mobile devices, or share them over the phone. If you must store passwords electronically, do so with a password manager that has been approved by IT. If you truly must share a password, do so through a designated password manager or grant access to an application through a single sign on provider.

iii. Do not use the “Remember Password” feature of applications and web browsers.

iv. If you suspect a password has been compromised, rotate the password immediately and notify engineering/security.

c. Enforcement

i. An employee or contractor found to have violated this policy may be subject to disciplinary action.

Policy
Training
Policy

D
O
L
P
H
I
N
I
N
C
J
u
l
y
2

Contents

0 1

2

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC9.9

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document

1 Purpose and Scope

a. This policy addresses policy education requirements for employees and contractors.

b. This policy applies to all full-time employees, part-time employees, and contractors. Adherence to assigned policies is binding under their Employment Offer Letter and/or Independent Contractor Agreement.

2 Applicability

a. Upon hire of a new employee or contractor, the Hiring Manager will determine which subsets of policies will apply to that individual. The individual will have five working days to read the assigned policies. The following will be logged in the Policy Training Policy Ledger:

    i. Assignment date

    ii. Completion date

    iii. Policy

    iv. Assignee

    v. Assigner

    vi. Notes

Products and Services Narrative

DOLPHI

N INC

July 2021

Contents

Table 1: Document history

Date	Comment
Jun 1 2018	Initial document

1 Products Narrative

Here we describe the key products marketed by our organization

2 Products

2.1 Product 1

Overview of product 1

2.1.1 Architecture

Brief architectural discussion of product 1

2.1.2 Security Considerations

Specific security considerations for product 1. Refer to policies, procedures here.

3 References

3.1 Narratives

List relevant narratives, probably including Organizational Narrative Security Narrative System Narrative

3.2 Policies

List relevant policies, probably including Application Security Policy Datacenter Policy Log Management Policy Password Policy Security Incident Response Policy Risk Assessment Policy

3.3 Procedures

List relevant procedures, probably including access review, patching, alert monitoring, log review, pen testing

Processing Integrity Policy

DOLPHIN INC July 2020

Contents

2 1

1 Coming Soon **2**

Table 1: Control

satisfaction Standard Controls

Satisfied

TSC PI1.1, PI1.2, PI1.3, PI1.4, PI1.5

Table 2: Document
history DateComment

Jun 1 2018 Initial document

1 Coming Soon

Office Security Policy

DOLPHIN INC July 2020

Contents

2 1

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC6.4

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document

1 Purpose and Scope

a. This policy establishes the rules governing controls, monitoring, and removal of physical access to company's facilities.

b. This policy applies to all staff, contractors, or third parties who require access to any physical location owned, operated, or otherwise occupied by the company. A separate policy exists for governing access to the company data center.

2 Policy

a. Management responsibilities

i. Management shall ensure:

1. appropriate entry controls are in place for secure areas
2. security personnel, identification badges, or electronic key cards should be used to validate employee access to facilities
3. confirm visitor & guest access procedure has been followed by host staff
4. management periodically reviews list of individuals with physical access to facilities
5. card access records and visitor logs are kept for a minimum of 90 days and are periodically reviewed for unusual activity

b. Key access & card systems

i. The following policies are applied to all facility access cards/keys:

1. Access cards/keys shall not be shared or loaned to others
2. Access cards/keys shall not have identifying information other than a return mail address
3. Access cards/keys shall be returned to Human Resources when they are no longer needed
4. Lost or stolen access cards/keys shall be reported immediately
5. If an employee changes to a role that no longer requires physical access or leaves the company, their access cards/keys will be suspended
6. Human Resources will regularly review physical security privileges and review access logs

a. *Staff & contractor access procedure*

   i. Access to physical locations is granted to employees and contractors based on individual job function and will be granted by Human Resources.

   ii. Any individual granted access to physical spaces will be issued a physical key or access key card. Key and card issuance is tracked by Human Resources and will be periodically reviewed.

   iii. In the case of termination, Human Resources should ensure immediate revocation of access (i.e. collection of keys, access cards, and any other asset used to enter facilities) through the offboarding procedure.

b. *Visitor & guest access procedure*

   i. The following policies are applied to identification & authorization of visitors and guests:

      1. All visitors must request and receive written onsite authorization from a staff member.

      2. Visitor access shall be tracked with a sign in/out log. The log shall contain:visitor's name, firm represented, purpose of visit, and onsite personnel authorizing access

      3. The log shall be retained for a minimum of 90 days

      4. Visitors shall be given a badge or other identification that visibly distinguishes visitors from onsite personnel

      5. Visitor badges shall be surrendered before leaving the facility

c. *Audit controls & management*

   i. Documented procedures and evidence of practice should be in place for this policy. Acceptable controls and procedures include:

      1. visitor logs

      2. access control procedures

      3. operational key-card access systems

      4. video surveillance systems (with retrievable data)

      5. ledgers if issuing physical keys

d. *Enforcement*

   i. Employees, contractors, or third parties found in violation of this policy (whether intentional or accidental) may be subject to disciplinary action, including:

      1. reprimand

2. loss of access to premises
3. termination

Office Security Policy

Organizational Narrative

Contents

DOLPHIN INC
July 2

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC1.2, CC1.3, CC1.4, CC1.5, CC3.1, CC3.2, CC3.3

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document

1 Organizational Narrative

The following provides a description of the corporate a management structure of DOLPHIN INC.

The intent of this description is to establish both the legal jurisdiction and corporate cultural norms that serve as the foundation for DOLPHIN INC's compliance program.

2 Entity Type

DOLPHIN INC is a Delaware C-Corporation headquartered in San Francisco, California. DOLPHIN INC was established in 1970.

3 Integrity and Ethics

The Directors and Executives of DOLPHIN INC aspire to and demonstrate standards of ethics and integrity consistent with professional norms in American corporate environments.

Chief among these standards is a commitment to honesty in interactions with and among managers, directors, employees, contractors, customers, and other stakeholders.

4 Board Independence

The Board of Directors appoints and oversees the Chief Executive Officer (CEO).

5 Organizational Structure

DOLPHIN INC is composed of 7 primary divisions:

- Sales
- Marketing
- Manufacturing
- Research & Development
- Information Technology
- Human Resources
- Finance

Each division is led by a Vice President, who in turn reports to the CEO. A complete Organization Chart is maintained and distributed by Human Resources.

6 Management Objectives

Work is distributed to each division via Objectives set by the respective division Vice President, in collaboration with the Chief Executive Officer.

7 Risk to Objectives

DOLPHIN INC seeks to manage risk to Objectives through professional management strategies and tactics, including:

- Rigorous hiring practices
- Employee performance reviews
- Aligning compensation with objectives
- Regular communication of objectives by executive management

8 Fraud Risk to Objectives

DOLPHIN INC acknowledges the possibility that fraud may imperil corporate objectives. DOLPHIN INC undertakes various activities to manage fraud risk, including:

- Conducting regular financial audits
- Adhering to financial control principles
- Investigating suspicious transactions
- Performing criminal background checks on all employees
- Maximizing the use of information technology in fraud detection

Removable Media and Cloud Storage Policy

DOLPHI

N INC

July 2021

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC6.7

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document

Removable Media and Cloud Storage Policy

1 Purpose and Scope

a. This removable media, cloud storage and Bring Your Own Device (BYOD) policy defines the objectives, requirements and implementing instructions for storing data on removable media, in cloud environments, and on personally-owned devices, regardless of data classification level.

b. This policy applies to all information and data within the organization's information security program, as well as all removable media, cloud systems and personally-owned devices either owned or controlled by the organization.

c. This policy applies to all users of information systems within the organization. This typically includes employees and contractors, as well as any external parties that come into contact with systems and information controlled by the organization (hereinafter referred to as "users"). This policy must be made readily available to all users.

2 Background

a. This policy defines the procedures for safely using removable media, cloud storage and personally-owned devices to limit data loss or exposure. Such forms of storage must be strictly controlled because of the sensitive data that can be stored on them. Because each of these storage types are inherently ephemeral or portable in nature, it is possible for the organization to lose the ability to oversee or control the information stored on them if strict security standards are not followed.

b. This document consists of three sections pertaining to removable media, cloud storage, and personally-owned devices. Each section contains require- ments and implementing instructions for the registration, management, maintenance, and disposition of each type of storage.

c. Within this policy, the term sensitive information refers to information that is classified as RESTRICTED or CONFIDENTIAL in accordance with the Data Classification Policy (reference (a)).

3 References

a. Data Classification Policy

b. Asset Inventory

c. Security Incident Response Policy

d. Encryption Policy

4 Policy

a. Removable Media

i. All removable media in active use and containing data pertinent to the organization must be registered in the organization's Asset Inventory (reference (b)).

ii. All removable media listed in reference (b) must be re-inventoried on a quarterly basis to ensure that it is still within the control of the organization.

1. To re-inventory an item, the owner of the removable media must check in the item with the organization's Information Security Manager (ISM).

2. The ISM must treat any removable media that cannot be located as lost, and a security incident report must be logged in accordance with the Security Incident Response Policy (reference (c)).

iii. The owner of the removable media must conduct all appropriate maintenance on the item at intervals appropriate to the type of media, such as cleaning, formatting, labeling, etc.

iv. The owner of the removable media, where practical, must ensure that an alternate or backup copy of the information located on the device exists.

v. Removable media must be stored in a safe place that has a reduced risk of fire or flooding damage.

vi. If the storage item contains sensitive information, removable media must:

1. Be stored in a locked cabinet or drawer.

2. Store only encrypted data that is securely enciphered in accordance with the Encryption Policy (reference (d)).

vii. All data on removable media devices must be erased, or the device must be destroyed, before it is reused or disposed of.

viii. When removable media devices are disposed, the device owner must inform the ISM so that it can be removed from reference (b).

b. Cloud Storage

i. All cloud storage systems in active use and containing data pertinent to the organization must be registered in reference (b). Registration may be accomplished by manual or automated means.

ii. All cloud storage systems listed in reference (b) must be re-inventoried on a quarterly basis to ensure that it is still within the control of the

organization. To re-inventory an item, the owner of the removable media must check in the item with the organization's Information Security Manager (ISM). Re-inventory may be accomplished by manual or automated means.

iii. The owner of the cloud storage system must conduct all appropriate maintenance on the system at regular intervals to include system configuration, access control, performance monitoring, etc.

iv. Data on cloud storage systems must be replicated to at least one other physical location. Depending on the cloud storage provider, this replication may be automatically configured.

v. The organization must only use cloud storage providers that can demonstrate, either through security accreditation, demonstration, tour, or other means that their facilities are secured, both physically and electronically, using best practices.

vi. If the cloud storage system contains sensitive information, that information must be encrypted in accordance with reference (d).

vii. Data must be erased from from cloud storage systems using a technology and process that is approved by the ISM.

viii. When use of a cloud storage system is discontinued, the system owner must inform the ISM so that it can be removed from reference (b).

c. Personally-owned Devices

i. Organizational data that is stored, transferred or processed on personally-owned devices remains under the organization's ownership, and the organization retains the right to control such data even though it is not the owner of the device.

ii. The ISM is responsible for conducting overall management of personally-owned devices, to include:

1. Installation and maintenance of Mobile Device Management (MDM) software that can effectively manage, control and wipe data under the organization's control from personally-owned devices.

2. Maintain a list of job titles and/or persons authorized to use personally-owned devices for the organization's business, as well as the applications and databases that may be accessed from such devices.

3. Maintain a list of applications prohibited from use on personally-owned devices, and ensuring that device users are aware of these restrictions.

iii. Personally-identifiable information (PII) may not be stored, processed or accessed at any time on a personally-owned device.

iv. The following acceptable use requirements must be observed by users of personally-owned devices:

1. All organizational data must be backed up at regular intervals.
2. MDM and endpoint protection software must be installed on the device at all times.
3. Sensitive information stored on the device must be encrypted in accordance with reference (d).
4. The device must be secured using a password, pin, unlock pattern, fingerprint or equivalent security mechanism.
5. The device must only connect to secure and encrypted wireless networks.
6. When using the device outside of the organization's premises, it must not be left unattended, and if possible, physically secured.
7. When using the device in public areas, the owner must take measures to ensure that the data cannot be read or accessed by unauthorized persons.
8. Patches and updates must be installed regularly.
9. Classified information must be protected in accordance with reference (a).
10. The device owner must install the ISM before the device is disposed of, sold, or provided to a third party for servicing.
11. It is prohibited to:
    a. Allow device access for anyone except its owner.
    b. Store illegal materials on the device.
    c. Install unlicensed software.
    d. Locally-store passwords.
    e. Transfer organizational data to other devices which have not been approved by the organization.

v. The organization must reserve the right to view, edit, and/or delete any organizational information that is stored, processed or transferred on the device.

vi. The organization must reserve the right to perform full deletion of all of its data on the device if it considers that necessary for the

protection of company-related data, without the consent of the device owner.

vii. The organization will not pay the employees (the owners of BYOD) any fee for using the device for work purposes.

viii. The organization will pay for any new software that needs to be installed for company use.

ix. All security breaches related to personally-owned devices must be reported immediately to the ISM.

Log Management Policy

DOLPHIN INCJuly 2020

Contents

Removable Media and Cloud Storage Policy

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC7.2

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document

1 Purpose and Scope

a. This log management and review policy defines specific requirements for information systems to generate, store, process, and aggregate appropriate audit logs across the organization's entire environment in order to provide key information and detect indicators of potential compromise.

b. This policy applies to all information systems within the organization's production network.

c. This policy applies to all employees, contractors, and partners of the organization that administer or provide maintenance on the organization's production systems. Throughout this policy, these individuals are referred to as system administrators.

2 Background

a. In order to measure an information system's level of security through confidentiality, integrity, and availability, the system must collect audit data that provides key insights into system performance and activities. This audit data is collected in the form of system logs. Logging from critical systems, applications, and services provides information that can serve as a starting point for metrics and incident investigations. This policy provides specific requirements and instructions for how to manage such logs.

3 Policy

a. All production systems within the organization shall record and retain audit-logging information that includes the following information:
    i. Activities performed on the system.
    ii. The user or entity (i.e. system account) that performed the activity, including the system that the activity was performed from.
    iii. The file, application, or other object that the activity was performed on.
    iv. The time that the activity occurred.
    v. The tool that the activity was performed with.
    vi. The outcome (e.g., success or failure) of the activity.

b. Specific activities to be logged must include, at a minimum:
    i. Information (including authentication information such as usernames or passwords) is created, read, updated, or deleted.

ii. Accepted or initiated network connections.

iii. User authentication and authorization to systems and networks.

iv. Granting, modification, or revocation of access rights, including adding a new user or group; changing user privileges, file permis- sions, database object permissions, firewall rules, and passwords.

v. System, network, or services configuration changes, including software installation, patches, updates, or other installed software changes.

vi. Startup, shutdown, or restart of an application.

vii. Application process abort, failure, or abnormal end, especially due to resource exhaustion or reaching a resource limit or threshold (such as CPU, memory, network connections, network bandwidth, disk space, or other resources), the failure of network services such as DHCP or DNS, or hardware fault.

viii. Detection of suspicious and/or malicious activity from a security sys- tem such as an Intrusion Detection or Prevention System (IDS/IPS), anti-virus system, or anti-spyware system.

c. Unless technically impractical or infeasible, all logs must be aggregated in a central system so that activities across different systems can be correlated, analyzed, and tracked for similarities, trends, and cascading effects. Log aggregation systems must have automatic and timely log ingest, event and anomaly tagging and alerting, and ability for manual review.

d. Logs must be manually reviewed on a regular basis:

i. The activities of users, administrators and system operators must be reviewed on at least a monthly basis.

ii. Logs related to PII must be reviewed on at least a monthly basis in order to identify unusual behavior.

e. When using an outsourced cloud environment, logs must be kept on cloud environment access and use, resource allocation and utilization, and changes to PII. Logs must be kept for all administrators and operators performing activities in cloud environments.

f. All information systems within the organization must synchronize their clocks by implementing Network Time Protocol (NTP) or a similar capa- bility. All information systems must synchronize with the same primary time source.

Information Security Policy

DOLPHIN INC July 2020

Contents

2 1

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC9.9

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document

Information Security Policy

1 Purpose and Scope

a. This information security policy defines the purpose, principles, objectives and basic rules for information security management.

b. This document also defines procedures to implement high level information security protections within the organization, including definitions, procedures, responsibilities and performance measures (metrics and reporting mechanisms).

c. This policy applies to all users of information systems within the orga- nization. This typically includes employees and contractors, as well as any external parties that come into contact with systems and information controlled by the organization (hereinafter referred to as “users”). This policy must be made readily available to all users.

2 Background

a. This policy defines the high level objectives and implementation instruc- tions for the organization’s information security program. It includes the organization’s information security objectives and requirements; such objectives and requirements are to be referenced when setting detailed information security policy for other areas of the organization. This policy also defines management roles and responsibilities for the organization’s Information Security Management System (ISMS). Finally, this policy references all security controls implemented within the organization.

b. Within this document, the following definitions apply:

   i. *Confidentiality*: a characteristic of information or information systems in which such information or systems are only available to authorized entities.

   ii. *Integrity*: a characteristic of information or information systems in which such information or systems may only be changed by authorized entities, and in an approved manner.

   iii. *Availability*: a characteristic of information or information systems in which such information or systems can be accessed by authorized entities whenever needed.

   iv. *Information Security*: the act of preserving the confidentiality, in- tegrity, and, availability of information and information systems.

   v. *Information Security Management System (ISMS)*: the overall management process that includes the planning, implementation, maintenance, review, and, improvement of information security.

3 References

a. Encryption Policy
b. Data Center Security Policy
c. Disaster Recovery Policy
d. Password Policy
e. Remote Access Policy
f. Removable Media/Cloud Storage/BYOD Policy
g. Risk Assessment Policy
h. Security Incident Response Policy
i. Software Development Lifecycle Policy
j. System Availability Policy
k. Workstation Security Policy

4 Policy

a. Managing Information Security

i. The organization's main objectives for information security include the following:

1. [list the reasons/objectives for maintaining information security at the organization. Examples include a better market image, reduced risk of data breaches and compromises, and compliance with legal, regulatory, and contractual requirements.]

ii. The organization's objectives for information security are in line with the organization's business objectives, strategy, and plans.

iii. Objectives for individual security controls or groups of controls are proposed by the company management team, including but not lim- ited to [list key roles inside the organization that will participate in information security matters], and others as appointed by the CEO; these security controls are approved by the CEO in accordance with the Risk Assessment Policy (Reference (a)).

iv. All objectives must be reviewed at least once per year.

v. The company will measure the fulfillment of all objectives. The measurement will be performed at least once per year. The results must be analyzed, evaluated, and reported to the management team.

b. Information Security Requirements

Information Security Policy

i. This policy and the entire information security program must be compliant with legal and regulatory requirements as well as with contractual obligations relevant to the organization.

ii. All employees, contractors, and other individuals subject to the organization's information security policy must read and acknowledge all information security policies.

iii. The process of selecting information security controls and safeguards for the organization is defined in Reference (a).

iv. The organization prescribes guidelines for remote workers as part of the Remote Access Policy (reference (b)).

v. To counter the risk of unauthorized access, the organization maintains a Data Center Security Policy (reference (c)).

vi. Security requirements for the software development life cycle, including system development, acquisition and maintenance are defined in the Software Development Lifecycle Policy (reference (d)).

vii. Security requirements for handling information security incidents are defined in the Security Incident Response Policy (reference (e)).

viii. Disaster recovery and business continuity management policy is de- fined in the Disaster Recovery Policy (reference (f)).

ix. Requirements for information system availability and redundancy are defined in the System Availability Policy (reference (g)).

Datacenter Policy

D

O

L

P

H

I

N

I

N

C

J

u

l

y

2

0

Contents

Table 1: Control satisfaction

Standard	Controls
Satisfied TSC	CC6.4

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document

1 Purpose and Scope

a. The purpose of this policy is to define security procedures within the organization's data centers and secure equipment areas.

b. This policy applies to any cloud hosted providers and facilities within the organization that are labeled as either a data center or a secure equipment area. Such facilities are explicitly called out within this document.

c. This policy applies to all management, employees and suppliers that conduct business operations within cloud host or data centers and secure equipment areas.

2 Background

a. This policy defines the policies and rules governing data centers and secure equipment areas from both a physical and logical security perspective. The document lists all data centers and secure equipment areas in use by the organization, prescribes how access is controlled and enforced, and establishes procedures for any visitor or third party access. This policy also defines prohibited activities and requirements for periodic safety and security checks.

3 Policy

a. The following locations are classified by the organization as secure areas and are goverened by this policy:

    i. [list all data center locations and secure areas under the organization's control]

b. Each data center and secure area must have a manager assigned. The manager's name must be documented in the organization's records. In the case of any on-prem data centers, the manager's name must also be posted in and near the secure area.

c. Each secure area must be clearly marked. Access to the secure area must be controlled by at least a locked door. A visitor access log must be clearly marked and easily accessible just inside the door.

d. Persons who are not employed by the organization are considered to be visitors. Visitors accessing secure areas shall:

    i. Obtain access to secure areas in accordance with reference a.

ii. Only enter and remain in secure areas when escorted by a designated employee. The employee must stay with the visitor during their entire stay inside the secure area.

iii. Log the precise time of entry and exit in the visitor access log.

e. The following activities are prohibited inside secure areas:

i. Photography, or video or audio recordings of any kind.

ii. Connection of any electrical device to a power supply, unless specifi- cally authorized by the responsible person.

iii. Unauthorized usage of or tampering with any installed equipment.

iv. Connection of any device to the network, unless specifically authorized by the responsible person.

v. Storage or archival of large amounts of paper materials.

vi. Storage of flammable materials or equipment.

vii. Use of portable heating devices.

viii. Smoking, eating, or drinking.

f. Secure areas must be checked for compliance with security and safety requirements on at least a quarterly basis.

Cyber Risk Assessment Policy

Contents

D

O

L

P

H

I

N

I

N

C

J

u

l

y

2

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC9.1

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document

1 Purpose and Scope

a. The purpose of this policy is to define the procedures to assess and treat information security risks within the organization, and to define the acceptable level of risk overall.

b. Risk assessment and risk treatment are applied to the entire scope of the organization's information security program, and to all information systems which are used within the organization or which could have an impact on the organization's information security.

c. This policy applies to all management and employees that take part in the organization's risk assessments. This policy must be made readily available to all whom it applies to.

2 Background

a. This policy defines a step-by-step process for conducting risk assessments, as well as to treat identified risks from an information security perspective. This policy also describes how to prepare the Risk Assessment Report required as part of the risk assessment process.

b. When conducting a risk assessment, the organization must identify all organizational information systems . It must then identify all threats and vulnerabilities having to do with such systems , and rate the severity of such threats and vulnerabilities according to a predefined rating scale. Asset and risk owners must be defined for each risk item.

c. Once the risk assessment is completed, the organization shall determine how to manage risks where the overall assessed risk rating is deemed as too high. This management is known as risk treatment. Risk treatment options include but are not limited to applying security controls, outsourcing risk, accepting risk, or discontinuing the activity associated with the risk.

d. A penetration test must be performed by a third party to verify the accuracy of the risk assessment and effectiveness of deployed risk treatments.

3 Procedure To Execute Risk Assessment Re- port

a. Confirms that the entire risk assessment and risk treatment process has been carried out according to the Risk Assessment Policy.

b. The purpose of the risk assessment was to identify all information systems their vulnerabilities, and threats that could exploit vulnerabilities. These parameters were further evaluated in order to establish the criticality of individual risks.

c. The purpose of the risk treatment was to define the systematic means of reducing or controlling the risks identified in the risk assessment.

d. All risk assessment and treatment activities were completed within the scope of the organization's information security program.

e. The risk assessment was implemented in the period from [day/month/year] to [day/month/year]. The risk treatment was implemented from [day/month/year] to [day/month/year]. Final reports were prepared during [specify period].

f. The risk assessment and risk treatment process was managed by [person responsible for managing the risk assessment process] with expert assistance provided by [person or company responsible for assistance].

g. During the risk assessment, information was collected through question- naires and interviews with responsible persons, namely the asset owners across organizational units.

h. The process was conducted as follows:

    i. All information systems and their owners were identified.

    ii. Threats were identified for each asset, and corresponding vulnerabili- ties were identified for each threat.

    iii. Risk owners were identified for each risk.

    iv. Consequences of the loss of confidentiality, integrity and availability were evaluated using a score from 0 to 2, with 0 being the lowest rating and 2 being the highest rating.

    v. The likelihood of risk occurrence (i.e. that the threat will exploit the vulnerability) was evaluated using a score from 0 to 2, with 0 being the lowest rating and 2 being the highest rating.

    vi. The level of risk was calculated by adding up the consequence and likelihood.

    vii. Risks with a score of 3 or 4 were determined to be unacceptable risks.

    viii. For each unacceptable risk, a risk treatment option was considered, and appropriate information security controls were selected.

    ix. After controls were applied, residual risks were assessed.

i. The following documents were used or generated during the implementation of risk assessment and risk treatment:

    i. Risk Assessment Table (Appendix A): for each combination of sys- tems , vulnerabilities and threats, this table shows the values for consequence and likelihood, and calculates the risk.

ii. Risk Treatment Table (Appendix B): defines the options for risk treatment, selection of controls for each unacceptable risk, and the level of residual risk.

Confidentiality Policy

DOLPHIN INC July 2020

Contents

2 1

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	C1.1, C1.2

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document

1 Purpose and Scope

a. This policy outlines expected behavior of employees to keep confidential information about clients, partners, and our company secure.

b. This policy applies to all employees, board members, investors, and contractors, who may have access to confidential information. This policy must be made readily available to all whom it applies to.

2 Background

a. The company's confidential information must be protected for two reasons:
    i. It may be legally binding (i.e. sensitive customer data)
    ii. It may be fundamental to our business (i.e. business processes)

b. Common examples of confidential information in our company includes, but is not limited to:
    i. Unpublished financial information
    ii. Customer/partner/vendor/external party data
    iii. Patents, formulas, new technologies, and other intellectual property
    iv. Existing and prospective customer lists
    v. Undisclosed business strategies including pricing & marketing
    vi. Materials & processes explicitly marked as "confidential"

c. Employees will have varying levels of authorized access to confidential information.

3 Policy

a. Employee procedure for handling confidential information

i. Lock and secure confidential information at all times
    ii. Safely dispose (i.e. shred) documents when no longer needed
    iii. View confidential information only on secure devices
    iv. Disclose information only when authorized and necessary
    v. Do not use confidential information for personal gain, benefit, or profit
    vi. Do not disclose confidential information to anyone outside the com- pany or to anyone within the company who does not have appropriate privileges

vii. Do not store confidential information or replicates of confidential information in unsecured manners (i.e. on unsecured devices)

viii. Do not remove confidential documents from company's premises unless absolutely necessary to move

b. Offboarding measures

i. The Hiring Manager should confirm the off-boarding procedure has been completed by final date of employment.

c. Confidentiality measures

i. The company will take the following measures to ensure protection of confidential information:

1. Store and lock paper documents
2. Encrypt electronic information and implement appropriate technical measures to safeguard databases
3. Require employees to sign non-disclosure/non-compete agreements
4. Consult with senior management before granting employees access to certain confidential information

d. Exceptions

i. Under certain legitimate conditions, confidential information may need to be disclosed. Examples include:

1. If a regulatory agency requests information as part of an audit or investigation
2. If the company requires disclosing information (within legal bounds) as part of a venture or partnership

ii. In such cases, employee must request and receive prior written authorization from their hiring manager before disclosing confidential information to any third parties.

e. Disciplinary consequences

i. Employees who violate the confidentiality policy will face disciplinary and possible legal action.

ii. A suspected breach of this policy will trigger an investigation. Intentional violations will be met with termination and repeated unintentional violations may also face termination.

iii. This policy is binding even after the termination of employment.

Code of Conduct Policy

DOLPHIN INCJuly 2021

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC1.1

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document

Code of Conduct Policy

1 Purpose and Scope

a. The purpose of this policy is to define expected behavior from employees towards their colleagues, supervisors, and the overall organization.

b. We expect all employees to follow our Code of Conduct. Offensive behavior, disruptive behavior, and participation in serious disputes should be avoided. Employees are expected to foster a respectful and collaborative environment.

c. This policy applies to all employees and contractors. They are bound by their Employment Offer Letter or Independent Contractor Agreement to follow the Code of Conduct Policy while performing their duties. The Code of Conduct is outlined below:

#Policy

a. Compliance with law

i. Employees should have an understanding of and comply with all environmental, safety, and fair dealing laws. When performing their job duty and dealing with the company's products, finances, critical information, & public image, employees are expected to be ethical and responsible. If an employee is unsure of whether a contemplated action is permitted by law or Company policy, they should seek advice from the resource manager.

b. Respect in the workplace

i. Employees should respect their colleagues. Discriminatory behavior, harassment, or victimization will not be tolerated.

c. Protection of company property

i. Company property, both material or intangible, should be treated with respect and care. Employees and contractors:

1. Should not misuse company equipment
2. Should respect all intangible property, including trademarks, copyright, information, reports, and other property. These materials should be used only to complete job duties.
3. Should protect company facilities and other material property from damage and vandalism, whenever possible.

a. *Personal appearance*

    i. When in the workplace, employees must present themselves in an appropriate & professional manner. They should abide by the company dress code.

b. *Corruption*

    i. Employees are discouraged from accepting gifts from clients or partners. Briberies are prohibited for the benefit of any external or internal party.

c. *Job duties and authority*

    i. Employees should fulfill their job duties with integrity and respect towards all individuals involved.

    ii. Supervisors and managers may not use abuse their authority. Competency and workload should be taken into account when delegating duties to team members.

    iii. Team members are expected to follow their leaders' instructions and complete their duties with thoughtfulness and in a timely manner.

d. *Absenteeism and tardiness*

    i. Employees should be punctual when coming to and leaving from work and follow the schedule determined by their hiring manager. Exceptions can be made for occasions that prevent employees from following standard working hours or days, with approval from their hiring manager.

e. *Conflict of interest*

    i. Employees should avoid any personal, financial, or other interests that might compete with their job duties.

f. *Collaboration*

    i. Employees should be friendly with their colleagues and open to collab- oration. They should not disrupt the workplace or present obstacles to their colleagues' work.

g. *Communication*

    i. Colleagues, supervisors, or team members must be open to communication amongst each other.

h. *Benefits*

    i. We expect employees to not abuse their employment benefits. This can refer to time off, insurance, facilities, subscriptions, or other benefits our company offers. Refer to Human Resources for more information on benefits.

Code of Conduct Policy

i. *Policies*

i. All employees must comply with company policies. Questions should be directed to their hiring managers and/or Human Resources.

j. *Disciplinary actions*

i. Repeated or intentional violation of the Code of Conduct Policy will be met with disciplinary action. Consequences will vary depending on the violation, but can include:

1. demotion
2. reprimand
3. suspension or termination
4. detraction of benefits for a definite or indefinite time

ii. Cases of corruption, theft, embezzlement, or other unlawful behavior may call for legal action.

Control Environment Narrative

D

O

L

P

H

I

N

I

N

C

J

u

l

y

2

0

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC2.1, CC2.2, CC2.3, CC4.1, CC4.2, CC5.1, CC5.2, CC5.3

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document

1 Control Environment Narrative

The following provides a description of the control structure of DOLPHIN INC.

The intent of this description is to enumerate the logical, policy, and procedural controls that serve to monitor DOLPHIN INC's application and data security. Changes uncovered by these procedures in the logical, policy, procedural, or customer environment are addressed by remediations specific to the noted change.

2 Logical Controls

DOLPHIN INC employs several logical controls to protect confidential data and ensure normal operation of its core product.

- Mandatory data encryption at rest and in motion
- Multi-factor authentication for access to cloud infrastructure
- Activity and anomaly monitoring on production systems
- Vulnerability management program

3 Policy Controls

DOLPHIN INC employs several policy controls to protect confidential data and ensure normal operation of its core product. These policies include, but are not limited to:

- Access Control Policy
- Encryption Policy
- Office Security Policy
- Password Policy
- Policy Training Policy
- Vendor Policy
- Workstation Policy

4 Procedural Controls

DOLPHIN INC has numerous scheduled procedures to monitor and tune the effectiveness of ongoing security controls, and a series of event-driven procedures to respond to security-related events.

TODO: Finalize these lists

4.1 Scheduled Security and Audit Procedures

- Review Access [quarterly]
- Review Security Logs [weekly]

- Review Cyber Risk Assessment (enumerate possible compromise scenarios) [quarterly]
- Review Data Classification [quarterly]
- Backup Testing [quarterly]
- Disaster Recovery Testing [semi-annual]
- Review Devices & Workstations [quarterly]
- Review & Clear Low-Priority Alerts [weekly]
- Apply OS Patches [monthly]
- Verify Data Disposal per Retention Policy [quarterly]
- Conduct Security Training [annual]
- Review Security Monitoring and Alerting Configuration [quarterly]
- Penetration Test [annual]
- Whitebox Security Review [annual]
- SOC2 Audit [annual]

4.2 Event-Driven Security and Audit Procedures

- Onboard Employee
- Offboard Employee
- Investigate Security Alert
- Investigate Security Incident

5 Remediations

DOLPHIN INC uses the outcomes of the aforementioned controls and procedures to identify shortcomings in the existing control environment. Once identified, these shortcomes are remediated by improving existing controls and procedures, and creating new controls and procedures as needed.

6 Communications

DOLPHIN INC communicates relevant information regarding the functioning of the above controls with internal and external parties on an as-needed basis and according to statutory requirements.

6.1 Internal

DOLPHIN INC communicates control outcomes, anomalies, and remediations internally using the following channels:

- Slack
- Email
- Github ticketing

6.2 External

DOLPHIN INC communicates relevant control-related information to external parties including shareholders, customers, contractors, regulators, and government entities as needed according to contractual and regulatory/statutory obligation.

Business Continuity Policy

D

O

L

P

H

I

N

I

N

C

J

u

l

y

2

0

2

1

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC9.1

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document

Business Continuity Policy

1 Purpose and Scope

a. The purpose of this policy is to ensure that the organization establishes objectives, plans and, procedures such that a major disruption to the organization's key business activities is minimized.

b. This policy applies to all infrastructure and data within the organization's information security program.

c. This policy applies to all management, employees, and suppliers that are involved in decisions and processes affecting the organization's business continuity. This policy must be made readily available to all whom it applies to.

2 Background

a. The success of the organization is reliant upon the preservation of critical business operations and essential functions used to deliver key products and services. The purpose of this policy is to define the criteria for continuing business operations for the organization in the event of a disruption. Specifically, this document defines:

   i. The structure and authority to ensure business resilience of key processes and systems.

   ii. The requirements for efforts to manage through a disaster or other disruptive event when the need arises.

   iii. The criteria to efficiently and effectively resume normal business operations after a disruption.

b. Within this document, the following definitions apply:

   i. *Business impact analysis/assessment* - an exercise that determines the impact of losing the support of any resource to an enterprise, establishes the escalation of that loss over time, identifies the mini- mum resources needed to return to a normal level of operation, and prioritizes recovery of processes and the supporting system.

   ii. *Disaster recovery plan* - a set of human, physical, technical, and procedural resources to return to a normal level of operation, within a defined time and cost, when an activity is interrupted by an emergency or disaster.

   iii. *Recovery time objective* - the amount of time allowed for the recovery of a business function or resource to a normal level after a disaster or disruption occurs.

   iv. *Recovery point objective* - determined based on the acceptable data loss in the case of disruption of operations.

3 Policy

a. Business Risk Assessment and Business Impact Analysis

i. Each manager is required to perform a business risk assessment and business impact analysis for each key business system within their area of responsibility.

ii. The business risk assessment must identify and define the criticality of key business systems and the repositories that contain the relevant and necessary data for the key business system.

iii. The business risk assessment must define and document the Disaster Recovery Plan (DRP) for their area of responsibility. Each DRP shall include:

1. Key business processes.
2. Applicable risk to availability.
3. Prioritization of recovery.
4. Recovery Time Objectives (RTOs).
5. Recovery Point Objectives (RPOs).

b. Disaster Recovery Plan

i. Each key business system must have a documented DRP to provide guidance when hardware, software, or networks become critically dysfunctional or cease to function (short and long term outages).

ii. Each DRP must include an explanation of the magnitude of infor- mation or system unavailability in the event of an outage and the process that would be implemented to continue business operations during the outage. Where feasible, the DRP must consider the use of alternative, off-site computer operations (cold, warm, hot sites).

iii. Each plan must be reviewed against the organization's strategy, objectives, culture, and ethics, as well as policy, legal, statutory and regulatory requirements.

iv. Each DRP must include:

1. An emergency mode operations plan for continuing operations in the event of temporary hardware, software, or network outages.
2. A recovery plan for returning business functions and services to normal on-site operations.
3. Procedures for periodic testing, review, and revisions of the DRP for all affected business systems, as a group and/or individually.

c. Data Backup and Restoration Plans

Business Continuity Policy

i. Each system owner must implement a data backup and restoration plan.

ii. Each data backup and restoration plan must identify:

    1. The data custodian for the system.
    2. The backup schedule of each system.
    3. Where backup media is to be stored and secured, as well as how access is maintained.
    4. Who may remove backup media and transfer it to storage.
    5. Appropriate restoration procedures to restore key business system data from backup media to the system.
    6. The restoration testing plan and frequency of testing to confirm the effectiveness of the plan.
    7. The method for restoring encrypted backup media.

Application Security Policy

D

O

L

P

H

I

N

I

N

C

J

u

l

y

2

0

2

1

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC6.2

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document

Application Security Policy

1 Purpose and Scope

a. This application security policy defines the security framework and require- ments for applications, notably web applications, within the organization's production environment.

b. This document also provides implementing controls and instructions for web application security, to include periodic vulnerability scans and other types of evaluations and assessments.

c. This policy applies to all applications within the organization' production environment, as well as administrators and users of these applications. This typically includes employees and contractors.

2 Background

a. Application vulnerabilities typically account for the largest number of initial attack vectors after malware infections. As a result, it is important that applications are designed with security in mind, and that they are scanned and continuously monitored for malicious activity that could indicate a system compromise. Discovery and subsequent mitigation of application vulnerabilities will limit the organization's attack surface, and ensures a baseline level of security across all systems.

b. In addition to scanning guidance, this policy also defines technical require- ments and procedures to ensure that applications are properly hardened in accordance with security best practices.

3 References

a. Data Classification Policy

b. OWASP Risk Rating Methodology

c. OWASP Testing Guide

d. OWASP Top Ten Project

4 Policy

a. The organization must ensure that all applications it develops and/or acquires are securely configured and managed.

b. The following security best practices must be considered and, if feasible, applied as a matter of the application's security design:

    i. Data handled and managed by the application must be classified in accordance with the Data Classification Policy (reference (a)).

ii. If the application processes confidential information, a confidential record banner must be prominently displayed which highlights the type of confidential data being accessed (e.g., personally-identifiable information (PII), protected health information (PHI), etc.)

iii. Sensitive data, especially data specifically restricted by law or policy (e.g., social security numbers, passwords, and credit card data) should not be displayed in plaintext.

iv. Ensure that applications validate input properly and restrictively, allowing only those types of input that are known to be correct. Examples include, but are not limited to cross-site scripting, buffer overflow errors, and injection flaws.

v. Ensure that applications execute proper error handling so that errors will not provide detailed system information to an unprivileged user, deny service, impair security mechanisms, or crash the system.

vi. Where possible, authorize access to applications by affiliation, member- ship or employment, rather than by individual. Provide an automated review of authorizations on a regular basis, where possible.

vii. Ensure that applications encrypt data at rest and in transit.

viii. Implement application logging to the extent practical. Retain logs of all users and access events for at least 14 days.

ix. Qualified peers conduct security reviews of code for all new or significantly modified applications; particularly, those that affect the collection, use, and/or display of confidential data. Document all actions taken.

x. Implement a change management process for changes to existing software applications.

xi. Standard configuration of the application must be documented.

xii. Default passwords used within the application, such as for administrative control panels or integration with databases must be changed immediately upon installation.

xiii. Applications must require complex passwords in accordance with current security best practices (at least 8 characters in length, combi- nation of alphanumeric upper/lowercase characters and symbols).

xiv. During development and testing, applications must not have access to live data.

c. Where applications are acquired from a third party, such as a vendor:

i. Only applications that are supported by an approved vendor shall be procured and used.

ii. Full support contracts must be arranged with the application vendor for full life-cycle support.

iii. No custom modifications may be applied to the application without confirmation that the vendor can continue to provide support.

iv. Updates, patches and configuration changes issued by the vendor shall be implemented as soon as possible.

v. A full review of applications and licenses shall be completed at least annually, as part of regular software reviews.

d. Web applications must be assessed according to the following criteria:

i. New or major application releases must have a full assessment prior to approval of the change control documentation and/or release into the production environment.

ii. Third-party or acquired applications must have a full assessment prior to deployment.

iii. Software releases must have an appropriate assessment, as determined by the organization's information security manager, with specific evaluation criteria based on the security risks inherent in the changes made to the application's functionality and/or architecture.

iv. Emergency releases may forego security assessments and carry the assumed risk until a proper assessment can be conducted. Emergency releases must be approved by the Chief Information Officer or designee.

e. Vulnerabilities that are discovered during application assessments must be mitigated based upon the following risk levels, which are based on the Open Web Application Security Project (OWASP) Risk Rating Methodology (reference (b)):

i. High - issues categorized as high risk must be fixed immediately, otherwise alternate mitigation strategies must be implemented to limit exposure before deployment. Applications with high risk issues are subject to being taken off-line or denied release into the production environment.

ii. Medium - issues categorized as medium risk must be reviewed to determine specific items to be mitigated. Actions to implement mitigations must be scheduled. Applications with medium risk issues may be taken off-line or denied release into the production environment based on the number of issues; multiple issues may increase the risk to an unacceptable level. Issues may be fixed in patch releases unless better mitigation options are present.

iii. Low - issues categorized as low risk must be reviewed to determine specific items to be mitigated. Actions to implement mitigations

Application Security Policy
must be scheduled.

f. Testing is required to validate fixes and/or mitigation strategies for any security vulnerabilities classified as Medium risk or greater.

g. The following security assessment types may be leveraged to perform an application security assessment:

   i. Full - comprised of tests for all known web application vulnerabilities using both automated and manual tools based on the OWASP Test- ing Guide (reference (c)). A full assessment must leverage manual penetration testing techniques to validate discovered vulnerabilities to determine the overall risk of any and all discovered issues.

   ii. Quick - consists of an automated scan of an application for, at a min- imum, the OWASP Top Ten web application security risks (reference (d)).

   iii. Targeted - verifies vulnerability remediation changes or new applica- tion functionality.

   iv. To counter the risk of unauthorized access, the organization maintains a Data Center Security Policy (reference (c)).

   v. Security requirements for the software development life cycle, including system development, acquisition and maintenance are defined in the Software Development Lifecycle Policy (reference (d)).

   vi. Security requirements for handling information security incidents are defined in the Security Incident Response Policy (reference (e)).

   vii. Disaster recovery and business continuity management policy is de- fined in the Disaster Recovery Policy (reference (f)).

   viii. Requirements for information system availability and redundancy are defined in the System Availability Policy (reference (g)).

Access Onboarding and Termination Policy

DOLPHI

N INC

July 2021

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied TSC
CC6.1, CC6.2, CC6.3	

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document

1 Purpose and Scope

a. The purpose of this policy is to define procedures to onboard and offboard users to technical infrastructure in a manner that minimizes the risk of information loss or exposure.

b. This policy applies to all technical infrastructure within the organization.

c. This policy applies to all full-time and part-time employees and contractors.

2 Background

a. In order to minimize the risk of information loss or exposure (from both inside and outside the organization), the organization is reliant on the principle of least privilege. Account creation and permission levels are restricted to only the resources absolutely needed to perform each person's job duties. When a user's role within the organization changes, those accounts and permission levels are changed/revoked to fit the new role and disabled when the user leaves the organization altogether.

3 Policy

a. During onboarding:

i. Hiring Manager informs HR upon hire of a new employee.

ii. HR emails IT to inform them of a new hire and their role.

iii. IT creates a checklist of accounts and permission levels needed for that role.

iv. The owner of each resource reviews and approves account creation and the associated permissions.

v. IT works with the owner of each resource to set up the user.

b. During offboarding:

i. Hiring Manager notifies HR when an employee has been terminated.

ii. HR sends a weekly email report to IT summarizing list of users terminated and instructs IT to disable their access.

iii. IT terminates access within five business days from receipt of notification.

c. When an employee changes roles within the organization:

i. Hiring Manager will inform HR of a change in role.

ii. HR and IT will follow the same steps as outlined in the onboarding and offboarding procedures.

d. Review of accounts and permissions:

i. Each month, IT and HR will review accounts and permission levels for accuracy.

DOLPHIN INC PRIVACY POLICY

DOLPHIN INC, Inc. and its affiliates worldwide ("**DOLPHIN INC**" or **"we"** or **"us"**) are committed to protecting the privacy of the users (**"you"** or **"user"**) of its Internet websites and applications, and the related services we provide through the Internet, in person,
through the telephone or through use of electronic communications (individually and collectively, the **"Services"**).

This Privacy Policy, together with our Cookies Policy, describes our practices regarding the Personal Data we collect from you when you use the Services. As used in this Privacy Policy, **"Personal Data"** means data that allows someone to identify or contact you (for example, your name, address, telephone number and e-mail address) and any other non-public information about you that is associated with or linked to such data.

If you have any concerns or questions about your privacy or use of our Services, please contact us as provided below in the section "How to Contact Us."

1. **CONSENT**. ***By submitting Personal Data through our Services, you agree to the terms of this Privacy Policy and you consent to the use of your Personal Data in accordance with this Privacy Policy.***

2. **CHANGES TO THIS PRIVACY POLICY**. This Privacy Policy is subject to occasional revision. We encourage you to visit this page regularly to view our current Privacy Policy, which will indicate the date of the last change. If we make any substantial changes in the way we use your Personal Data, we will notify you by prominently posting notice of the updated Privacy Policy on this page, together with its effective date, and will notify users as required by law. Continued use of our Services, after we have posted changes on this page and with a new effective date shall indicate your acknowledgement of such changes and your agreement to be bound by the terms and conditions of such changes. If you do not wish to permit changes in our use of your Personal Data, you must notify us prior to the effective date of the changes that you wish to deactivate your account with us and you should cease further use of our Services.
3. **CHILDREN UNDER 13**. Children under the age of 13 should not send us Personal Data. We do not knowingly collect any Personal Data from children who are under the age of 13. If we become aware that an individual under the age of 13 is submitting information to us, we will attempt to delete the information as soon as possible.
4. **CONSENT TO INTERNATIONAL TRANSFERS OF INFORMATION**. Your Personal Data may be processed in the country in which it was collected and in other countries or jurisdictions that may not have the same data protection laws, or provide as much protection to Personal Data, as the country where you reside. By using the Services, you consent to the transfer and storage of your Personal Data to any other country in which we or our service providers maintain facilities.

5. **TYPES OF DATA WE COLLECT**. We collect both Personal Data and Anonymous Data from you when you use our Services or when you send us information or communications. **"Anonymous Data"** means data that is not associated with or linked to Personal Data and does not permit the identification of individual persons. We collect Personal Data and Anonymous Data, as described below.

5.1 **Personal Data You Provide to Us**. If you provide us feedback or contact us via e-mail or through our Services (e.g., in response to a posted employment opportunity), we will collect your name and e-mail address, as well as any other content included in the feedback or e-mail, in order to send you a reply. When you participate in one of our surveys, request information or establish an account with us, we may collect additional profile information. We do not collect your name, address, telephone number, e-mail address or other contact information unless you choose to provide that information.

5.2 **Personal Data Collected through Technology**. Our computer systems (or those of our service providers) may electronically collect information about you when you use our Services. The information collected may be machine generated and may include, for example, the domain name of your Internet provider, your browser type, time zone, language, operating system, date of the visit, URL of the last webpage visited before visiting our Website, and URL of the first page you visit after leaving our Website, pages viewed, time spent on a page, click through and clickstream data, queries made, search results selected, history, or comments made. When we send you an electronic communication, such as an e-mail, we may collect certain information, such as the action taken upon receipt of the e-mail (for instance, whether you opened or deleted the e-mail).

Our Services use cookies and similar technologies (e.g., web beacons, pixels and device identifiers) to store on a user's computer or device information about the user's identity and preferences and settings, to gather statistical information about the use of our Services, to improve the design and functionality of our Services. Please review our Cookie Policy for further information about how we use cookies and how you can disable them.

We use Google Analytics, which uses cookies and similar technologies to collect and analyze information about the use of our Services, and report on the activities and trends. You can learn about Google's practices by going to www.google.com/policies/privacy/partners. You may opt-out from the collection of your information by downloading the Google Analytics opt-out browser add-on available at https://tools.google.com/dlpage/gaoptout.

5.3 **Personal Data Collected from Third Parties.** We may obtain information from third parties with whom we do business, such as in connection with a trade show or webinar or through public databases, social media or joint marketing partners.

6. **USE OF YOUR DATA**.

6.1 **General Use**. We use Personal Data collected from users for the following purposes:

- To provide the Services requested by a user.
- To respond to user questions and other requests for information made through the Services.
- To forward administrative information to the user.
- To send marketing information, invitations to events or other communications that we believe may be of interest to the user.
- To keep records of contact information and correspondence.
- To remember a user's preferences, such as language, font size and communication type, and the user's interests regarding subject matter.
- To personalize a user's online experience, including the provision of content addressing a user's preferences or interests and expediting the processing and completion of a transaction.
- To administer our Services, diagnose technical problems, and otherwise manage our business.
- To allow a user to navigate or browse through our Services more quickly and efficiently.
- To determine the approximate location of each user, calculate usage levels, diagnose server problems, and in general to administer the Services, in each case through use of a user's IP address.
- To improve, enhance or modify our business and the Services through data analysis, audits, security and fraud monitoring and prevention.
- To aggregate information and create Anonymous Data, as described below.
- To perform other functions or processes described to the user at the time of collection of the Personal Data.

6.2 **Creation of Anonymous Data**. We may create Anonymous Data records from Personal Data by excluding information (such as your name) that make the data personally identifiable to you. We use this Anonymous Data to analyze request and usage patterns so that we may enhance the content of our Services and improve site navigation. We reserve the right to use and disclose Anonymous Data to third parties for research, analytic or strategic purposes.

6.3 **Feedback**. If you provide us with feedback on any of our Services, we may use such feedback for any purpose. We will treat the Personal Data in such communication in accordance with this Privacy Policy.

7. **DISCLOSURE OF YOUR PERSONAL DATA**.

7.1 **Affiliates**. We may share some or all of your Personal Data with our current and future subsidiaries, parent companies, or other companies that control or are under common control with us (our "Affiliates"), provided we require our Affiliates to honor this Privacy Policy. We also may share your Personal Data with our offices throughout the world, including in the United States, Europe and Asia.

7.2 **Change in Control or Sale.** We may transfer users' Personal Data to a successor entity in the event of a sale, merger, transfer or other disposition of all or any portion of our business, assets or ownership, or other change in control. Except as otherwise provided by a bankruptcy or other court, the use and disclosure of all transferred Personal Data will be subject to policies that are consistent with the policies described in this Privacy Policy. However, any information that a user submits or that is collected after that transaction may be subject to the privacy policy adopted by the successor entity.

7.3 **Legal Requests and Prevention of Harm.** We may use, share or disclose information about users, including your Personal Data, in order to address legal concerns or liabilities, particularly when we believe that a user has violated the *Terms of Use* of our Services or otherwise misused our Services, such as to gain unauthorized access to any system, to engage in spamming activities, to engage in denial of service or similar attacks, or to conduct any fraudulent or unlawful activity. We also may be required to provide legal authorities access to a user's information, in accordance with applicable law, including laws outside the user's country of residence.

7.4 **Disclosure to Third Party Service Providers**. Except as otherwise stated in this policy, we do not generally sell, trade, share, or rent the Personal Data collected from our Services to other entities. However, we may share your Personal Data with third party service providers to provide you with the Services; to conduct quality assurance testing; to facilitate creation of accounts; or to provide technical support. These third party service providers are contractually required not to use your Personal Data other than to provide the services we request. You expressly consent to the sharing of your Personal Data with our third party service providers for the sole purpose of providing the Services.

7.5 **Disclosure for Direct Marketing Purposes**. We currently do not share Personal Data with third parties for their direct marketing purposes without the express consent of the user.

7.6 **Social Media.** The Services may provide links to third party social media services (e.g., LinkedIn and Facebook) where a user is able to post comments. These third party services may collect, retain and share information about a user, and use of such third party services is subject to the terms and conditions of their privacy policies. Please note that any information that is posted or disclosed through social media may be available to us, to other users of that service or to the public. We recommend caution when using these features.

7.7 **Third Party Links.** The Services may contain links to third party websites to provide additional information or for the purposes of communication with such third parties. We are not responsible for the privacy policies of those third parties, and strongly encourage you to read and understand their privacy policies.

8. **YOUR CHOICES REGARDING YOUR PERSONAL DATA**.

8.1 **Opt Out From Communication**. We may periodically send you free newsletters and e-mails that directly promote the use of our Services and potentially those of our marketing partners. When you receive newsletters or promotional communications from us, you may indicate a preference to stop receiving further communications from us and you will have the opportunity to "opt-out" by following the unsubscribe instructions provided in the e-mail you receive or by contacting us directly (please see contact information below). Despite your indicated e-mail preferences, we may send you notices of any updates to our Terms of Use or Privacy Policy.

8.2 **Changes to and Deletion of Personal Data**. You may request that we change or delete any of your Personal Data in your account by sending an e-mail to us at the e-mail address set forth below. However, we may be required (by law or otherwise) to retain this information and not delete it (or to retain this information for a certain time period, in which case we will comply with your deletion request only after we have fulfilled such requirements). In regions where there is a right to erasure (right to be forgotten) with respect to your Personal Data, we will use all reasonable efforts to delete such Personal Data without undue delay. When we delete any information, it will be deleted from the active database, but may remain in our archives.

9. **SECURITY OF YOUR PERSONAL DATA**. We use a variety of technical, organizational and administrative measures to protect user information that we possess against unauthorized or unlawful access or processing, and against accidental loss, destruction or damage, We believe that these measures are reasonably adapted to the nature and types of information in our custody, However, even though we take reasonable efforts to protect the information in our custody, no transmission over the Internet and no data storage or security system is fully secure. Therefore, we cannot guarantee the security of any information that we may receive from you or transmit to you.
10. **RETENTION OF YOUR PERSONAL DATA.** We retain information about users or as long as necessary to perform the activities described in this Privacy Policy and to comply with our legal obligations. We may need to retain certain information for record keeping purposes or for completing a transaction that you commenced prior to requesting a change or deletion. In addition, it is likely that residual information may remain within our databases, back-ups or other records, and not be fully removed.
11. **DO NOT TRACK SIGNALS.** Some browsers give individuals the ability to communicate that they wish not to be tracked while browsing on the Internet. The Internet industry has not yet agreed on a definition of what "Do Not Track" means, how compliance with "Do Not Track" would be measured or evaluated, or a common approach to responding to a "Do Not Track" signal. Consequently, due to the lack of guidance, we have not yet developed features that would recognize or respond to browser-initiated Do Not Track signals in response to the laws of California or any other jurisdiction.
12. **CONTACT INFORMATION**. We welcome your comments or questions regarding this Privacy Policy. Please e-mail us at privacy@DOLPHIN INC.com. If you prefer to contact us by mail, please use the following address:

If you are located in the European Union or United Kingdom:

DOLPHIN INC Europe UK Office 1, Trafalgar Square, Northumberland Ave, London

WC2N If you are located in any country other than the countries listed above:

DOLPHIN INC, Inc., Attn: Data Protection Officer, 207 Powell Street, Suite 800,
San Francisco, CA 94102, USA

13. **DISPUTE RESOLUTION.**If you believe that we have not adhered to this Privacy Policy, please contact us by email at privacy@DOLPHIN INC.com. We will do our best to address your concerns. If you feel that your complaint has been addressed incompletely, we invite you to let us know for further investigation.

This Privacy Policy was last revised on May 25, 2018.

Data Protection Policy

Revised March 2023

Data Protection and Security

DOLPHIN INC, Inc. together with its affiliates (“DOLPHIN INC”) takes the protection and security of the data that it collects and holds, including personal data, very seriously. The policies outlined in this document are intended to inform and educate DOLPHIN INC’s employees, customers, and stakeholders regarding DOLPHIN INC’s general data protection and security policies and practices, but does not cover all scenarios. All DOLPHIN INC employees are expected to use good judgment in handling personal data and confidential or sensitive data, and to comply with the policies contained herein. If you have any questions about this Policy, or anything else relating to the handling and processing of data - contact DOLPHIN INC’s Data Protection Officer (“DPO”).

DOLPHIN INC’s policy regarding data security generally follows the NICE (National Institute of Cybersecurity Education) framework, published in conjunction with the National Institute of Standards and Technology. As a global company, DOLPHIN INC has made efforts to include best practices from the regions in which it operates both to put DOLPHIN INC in compliance with local law and to create a robust and feasible framework for managing the data of both DOLPHIN INC customers and employees.

Data Protection Officer

DOLPHIN INC’s DPO is responsible for developing, monitoring, and enforcing this Policy. This role reports directly into the CEO to minimize potential conflicts. Where appropriate, the DPO will offer suggestions and guidance on how to implement secure and appropriate data protection and security solutions.

In addition, the DPO is responsible for educating and training DOLPHIN INC staff on the Policy and their responsibilities under the rules and requirements in effect in their regions. Oversight of the application of the Policy to specific roles and functions may be delegated, but the DPO is expected to oversee such delegation and to be a resource in developing and applying policies in all appropriate functions within DOLPHIN INC.

The DPO also serves as a principal point of contact for any inquiries from external regulatory bodies or customers, and as a primary member of any investigation team related to potential breaches of data policies. The DPO will maintain comprehensive records of all investigations or complaints regarding DOLPHIN INC's data protection and security activities, as well as records of all training and consultation with respect to such activities. When requested by customers or appropriate third parties, the DPO will share relevant information about DOLPHIN INC's data usage to ensure compliance with regulatory restrictions or for other appropriate purposes.

Competencies

In order to implement and enforce this Policy, DOLPHIN INC has developed and will continue to develop key security competencies throughout its organization.

Competency	Description
Securely Provision (SP)	Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.
Operate and Maintain (OM)	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.
Oversee and Govern (OV)	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
Protect and Defend (PR)	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.
Analyze (AN)	Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.

Collect and Operate (CO)	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
Investigate (IN)	Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

All employees are responsible for exercising those security competencies relevant to their job responsibilities and the data with which they deal, and must actively participate in annual data protection training.

The DPO is responsible for maintaining and developing these competencies throughout DOLPHIN INC. The CTO, or someone designated by the CTO, will audit practices regularly to ensure that these competencies are being properly executed throughout DOLPHIN INC's organization.

Any questions regarding the proper exercise of data security competencies should be directed to the DPO.

Confidential Information

Confidential Information is any information which is not readily available through public sources. Generally, this will fall within the following categories:

Sensitive Employee Information
This is information about DOLPHIN INC employees or employees of our partners, customers, or contractors which is not generally available. Some common examples of employee information are:

- Personal Health Information (PHI) such as Diagnosis, Condition Status, Treating Physician, etc.
- Other sensitive personal information, such as race, gender, religion, sexual orientation and criminal record
- I-9 / Immigration Status
- Medical / Disability Status
- Salary or Compensation Information

This information is most often encountered by people in an HR Function, but customers may occasionally share this information with DOLPHIN INC for use within our products. At all

times this information must be treated as sensitive and confidential, and not disclosed to others (including within DOLPHIN INC) except as required to perform a necessary job function. Always assume that information of this nature is Confidential Information unless told otherwise.

Please review the DOLPHIN INC Data Protection Policy GDPR Addendum

DOLPHIN INC Information

This is information about DOLPHIN INC's business and products which is not generally available to those outside of DOLPHIN INC. As a private company, DOLPHIN INC may share its Confidential Information more broadly with its employees than some other companies. However, such information should never be disclosed to third parties, except under an approved Non-Disclosure Agreement and with appropriate approval of the Confidential Information to be disclosed. Even within DOLPHIN INC, unless disseminated by senior management, Confidential Information should only be shared on a "need to know basis." Some common examples of DOLPHIN INC information are:

- Financial information about DOLPHIN INC, including results and projections
- Identity and number of DOLPHIN INC's customers
- Details regarding how DOLPHIN INC's products work, including trade secrets and source code
- Details concerning DOLPHIN INC's sales negotiations
- DOLPHIN INC's product roadmap
- The identity of DOLPHIN INC's partners (to the extent not publicly disclosed) and details about DOLPHIN INC's relationship with those partners
- Details regarding internal operations

Customer/Third Party Information

This is information about DOLPHIN INC's customers or other third parties, which DOLPHIN INC receives from those third parties and which is shared solely for the purpose of facilitating an existing or potential customer engagement or other transaction. This information is likely to be exchanged among DOLPHIN INC employees during the process of negotiating or completing an engagement or other transaction, but should always be carefully monitored and managed to avoid sharing it with anyone not actively working on the project. Some common examples of Customer/Third Party information are:

- Whether someone is a customer
- Terms of the customer agreement
- Prescription or Market Share data
- Brand Strategies / Playbooks
- Customer deployment strategies and data

Personally Identifiable Information

Personally Identifiable Information (“PII”) is any information by which a specific individual may be identified, such as name, job title, phone number, email address and static IP address. Employees may come into contact with or collect PII of customers (“Customer PII”) in various dealings on behalf of DOLPHIN INC and should treat such Customer PII as confidential information, use it solely for business purposes and not disclose it outside of DOLPHIN INC.

Information Designated as Confidential

Anything marked as confidential should be treated as Confidential Information, regardless of the content, unless approval is obtained from the DPO to disregard such marking.

Data Security

DOLPHIN INC takes the privacy of its employees, customers and other business partners very seriously. This section outlines a series of safeguards that must be used in the protection of any Confidential Information.

Physical Security

As a general rule, DOLPHIN INC employees should avoid using physical media and creating physical copies of Confidential Information. The nature of the work done at DOLPHIN INC typically is conducted digitally; therefore much of DOLPHIN INC’s security infrastructure is focused on digital safeguards. However, when physical copies of Confidential Information are required, or physical devices are used, the following safeguards must be taken:

- Any storage of physical media, devices, or materials must be behind two locks. (For example, behind a locked entry door, and within a locked cabinet)
- DOLPHIN INC employees must not leave their laptops or tablets in the office or in any unsecure area.
- Any devices that contain Confidential Information must be secured in a locked container.
- Physical documents containing Confidential Information should be shredded once their use has been completed.
- Encrypt all physical media which will be used to store, transport, or share digital copies of Confidential Information. This includes the hard drive on all employee laptops.
- Use encrypted methods to transfer data between media and devices.

The best practice for DOLPHIN INC employees is to limit situations where physical safeguards are required. If an DOLPHIN INC employee requires assistance in how best to avoid creating

physical copies of Confidential Information, the employee should contact the CTO or the DPO.

Digital Security

Digital Security is a complex topic and best practices are continually evolving. However, there are basic digital security principles that DOLPHIN INC employees must be familiar with and follow. They are documented below.

Authentication and Authorization

All digital systems must use some form of authentication for access. This authentication comes in many forms – pin codes, passwords, biometrics, encrypted keys, etc – but is a baseline requirement for securing DOLPHIN INC's systems. As DOLPHIN INC uses a BYOD model for personal phones and related devices, this policy also applies to any personal device used by an employee which is able to access Confidential Information.

All usernames and passwords should be distinct to a specific user, with clear logging and records of authentication attempts stored in relevant systems. Where it is not possible to comply (for instance – with SalesForce credentials) credentials should be restricted to only those individuals who need access to complete their work and should be managed through an authenticated system which can be monitored.

DOLPHIN INC employees should not share authentication credentials to any system without appropriate authorization. If unsure, employees should check with the Chief Technology Officer for determining who has access to a system. The CTO will perform a regular audit of system access to ensure that only those who require access for work purposes have access to DOLPHIN INC systems.

Encryption

All Confidential Information must be encrypted for both storage and transmission. DOLPHIN INC uses encrypted technologies like Slack and Dropbox to facilitate this – all employees are encouraged to use these technologies to comply with this requirement.

Hardware Requirements

All DOLPHIN INC laptops are required to have encrypted hard drives.
Active, up-to-date virus detection and firewall software must be installed on all DOLPHIN INC laptops and systems.

Employee Compliance-

https://drive.google.com/file/d/1jDUwFtQpkI3T_2syKJ11jmuk_LoP5FHt/view

DOLPHIN INC takes the privacy of our employees and clients very seriously. To ensure that we are protecting our corporate and client data from security breaches, this policy must be followed and will be enforced to the fullest extent.
Scope

This policy applies to all data, but is not limited to electronic information found in email, databases, applications, and other media; paper information, such as hard copies of electronic data, employee files, internal memos, and so on. It is inclusive of data outside of DOLPHIN INC stored in a cloud service, and/or held on a mobile computing device.

This policy applies to staff who may be creators and/or users of such data. The policy also applies to third parties who access and use DOLPHIN INC systems and IT equipment or who create, process, or store data owned by DOLPHIN INC.
Audience.

This policy applies to all employees, management, contractors, vendors, business partners, and any other parties who have access to company data.

Data Classifications

DOLPHIN INC's data is comprised of four classifications of information:

1. Public/Unclassified. This is defined as information that is generally available to anyone within or outside of the company. Access to this data is unrestricted, may already be available and can be distributed as needed. Public/unclassified data includes, but is not limited to, marketing materials, annual reports, corporate financials, and other data as applicable. Employees may send or communicate a public/unclassified piece of data with anyone inside or outside of the company.

2. Private. This is defined as corporate information that is to be kept within the company. Access to this data may be limited to specific departments and cannot be distributed outside of the workplace. Private data includes, but is not limited to, work phone directories, organizational charts, company
policies, and other data as applicable.

All information not otherwise classified will be assumed to be Private. Employees may not disclose private data to anyone who is not a current employee of the company.

3. Confidential. This is defined as personal or corporate information that may be considered potentially damaging if released and is only accessible to specific groups [e.g. payroll, HR, etc.]. Confidential data includes, but is not limited to, social security numbers, contact information, tax forms, accounting data, security procedures [and other data as applicable].
DOLPHIN INC considers it a top priority to protect the privacy of our clients and employees.
A privacy policy, contained below, outlines our commitment to protecting personal data.
Employees may only share confidential data within the department or named distribution list.

4. Secret/Restricted. This is defined as sensitive data that, if leaked, would be harmful to DOLPHIN INC, its employees, contractors, and other parties as applicable. Access is limited to authorized personnel and third parties as required. Secret/restricted data includes, but is not limited to audit reports, legal documentation, business strategy details, and other data as Applicable.

Secret/restricted data cannot be disclosed by anyone other than the original author, owner or distributor.

It is the responsibility of everyone who works at DOLPHIN INC to protect our data. Even unintentional abuse of classified data will be considered punishable in accordance with the extent and frequency of the abuse.

Data that falls under Confidential and/or Secret/Restricted classifications must be encrypted while in transit and at rest. This includes data stored on corporate systems and mobile computing devices, including personal devices used to access corporate systems.

Responsibilities
All employees are responsible for adhering to the policy and reporting any activities that do not comply with this policy.
Management is responsible for ensuring that their direct reports understand the scope and implications of this policy. HR must also ensure that all employees have a signed copy of this policy in their file.
Management will be monitoring data for any unauthorized activity and are responsible for updating access requirements as needed.

Management
Ownership of this policy falls to the Compliance Committee. For any questions about this policy, or to report misuse of corporate or personal data, please contact him/her. The IT department will work in conjunction with Compliance Committee to maintain data access privileges, which will be updated as required when an employee joins or leaves the company.
These are the accepted technologies DOLPHIN INC used to enforce and ensure data security:
1. Access controls
2. Strong passwords
3. System monitoring
4. Intrusion detection software
5. Virus detection software Review
The Compliance Committee is responsible for keeping this policy current. This policy will be reviewed annually or as circumstances arise.
Enforcement
Employees found to be in violation of this policy by either unintentionally or maliciously stealing, using or otherwise compromising corporate or personal data may be subject to disciplinary action up to and including termination.

Administration

Oversight and Management

It is the responsibility of each DOLPHIN INC employee to handle Confidential Information responsibly. Any potential breach or violation of this Policy must be reported immediately to the DPO.

Each member of management must ensure that the manager's direct reports are provided with a copy of the Policy, complete required training and understand the requirements of this Policy. Any DOLPHIN INC employee that fails to complete the required training or demonstrates a lack of familiarity with the requirements of this Policy must promptly be brought to the attention of the DPO, who will address that gap.

The Data Protection Officer is the source of escalation for any questions or issues which arise from this Policy. The DPO is responsible for training, education, and enforcement of this Policy throughout DOLPHIN INC.

On termination of employment, all employee system accounts and access will be removed within 24 hours of the employee's termination.

Investigating potential incidents

Any potential security incident must be taken seriously, and acted upon with due urgency. When an incident is reported, it must be escalated immediately to the DPO, who will assign an incident manager ("Incident Manager") to make a preliminary determination as to the possibility of the breach and to perform the investigation outlined below.

Breaches of Confidential Information

In the event the Incident Manager determines that it is reasonably possible there has been a breach, there are specific steps that must be taken in response. These steps are not necessarily linear or comprehensive. Completion of one step is not required for others to start:

- Incident Manager creates an incident response team
- Incident response team determines the existence, scope and nature of the breach
- The Incident Manager or DPO oversees the notification of impacted parties
- The Incident Manager and DPO, in consultation with legal counsel, determine whether the breach also requires notifying governmental authorities.
- The incident response team builds an investigation strategy for the breach
- The incident response team collects and reviews data relevant to the breach
- The DPO, in consultation with the Incident Manager and appropriate members of senior management, determines and oversees implementation of appropriate remedial steps.

Contact

In case of any questions please reach out to:

DOLPHIN INC Chief Technology Officer (CTO): Dmitri.Daveynis@DOLPHIN INC.com