DevCare solutions

Information Security Program & Policies

Version 1.28

Last Update: 11/16/2019

For Internal Use Only

Contents

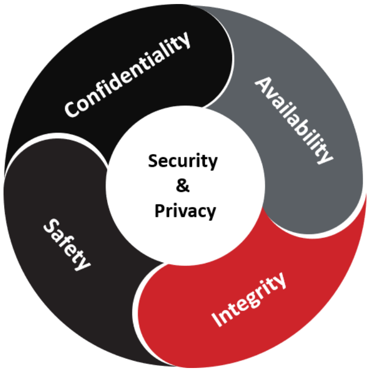
Information Security Program Overview

Introduction

The Written Information Security Program (WISP) provides definitive information on the prescribed measures used to establish and enforce the cybersecurity program at DEVCARE Solutions Ltd (DevCare).

Protecting DevCare data and the systems that collect, process and maintain this data is of critical importance. Therefore, the security of systems must include controls and safeguards to offset possible threats, as well as controls to ensure the confidentiality, availability and integrity of the data:

Commensurate with risk, cybersecurity and privacy measures must be implemented to guard against unauthorized access to, alteration, disclosure or destruction of data and systems. This also includes protection against accidental loss or destruction. The security of systems must include controls and safeguards to offset possible threats, as well as controls to ensure confidentiality, integrity, availability and safety:



CONFIDENTIALITY – Confidentiality addresses preserving restrictions on information access and disclosure so that access is limited to only authorized users and services.

INTEGRITY – Integrity addresses the concern that sensitive data has not been modified or deleted in an unauthorized and undetected manner.

AVAILABILITY – Availability addresses ensuring timely and reliable access to and use of information.

SAFETY – Safety addresses reducing risk associated with embedded technologies that could fail or be manipulated by nefarious actors.

Security measures must be taken to guard against unauthorized access to, alteration, disclosure or destruction of data and systems.
This also includes against accidental loss or destruction.

Purpose

The purpose of the Information Security Program (WISP) is to prescribe a comprehensive framework for:

- Protecting the confidentiality, integrity, and availability of DEVCARE data and systems;
- Protecting DEVCARE, its employees, and its clients from illicit use of DEVCARE systems and data.
- Ensuring the effectiveness of security controls over data and systems that support DEVCARE's operations.
- Recognizing the highly networked nature of the current computing environment and provide effective company-wide management and oversight of those related cybersecurity risks; and
- Providing for the development, review, and maintenance of minimum-security controls required to protect DEVCARE's data and systems.

The formation of these cybersecurity policies is driven by many factors, with the key factor being a risk. These policies set the ground rules under which DEVCARE operates and safeguards its data and systems to both reduce risk and minimize the effect of potential incidents.

Scope & Applicability

These policies, standards and guidelines apply to all DEVCARE data, systems, activities, and assets owned, leased, controlled, or used by DEVCARE, its agents, contractors, or other business partners on behalf of DEVCARE. These policies, standards and guidelines apply to all DEVCARE employees, contractors, sub-contractors, and their respective facilities supporting DEVCARE business operations, wherever DEVCARE data is stored or processed, including any third-party contracted by DEVCARE to handle, process, transmit, store, or dispose of DEVCARE data.

Some standards apply specifically to persons with a specific job function (e.g., a System Administrator); otherwise, all personnel supporting DEVCARE business functions shall comply with the standards. DEVCARE departments shall use these standards or may create a more restrictive standard, but none that are less restrictive, less comprehensive, or less compliant than these standards.

These policies do not supersede any other applicable law or higher-level company directive or existing labor management agreement in effect as of the effective date of this policy.

DEVCARE's documented cybersecurity roles & responsibilities provides a detailed description of DEVCARE user roles and responsibilities, regarding cybersecurity.

DEVCARE reserves the right to revoke, change, or supplement these policies, standards and guidelines at any time without prior notice.

Such changes shall be effective immediately upon approval by management unless otherwise stated.

Policy Overview

To ensure an acceptable level of cybersecurity risk, DEVCARE is required to design, implement and maintain a coherent set of policies, standards, procedures and guidelines to manage risks to its data and systems.

The WISP addresses the policies, standards and guidelines. Data/process owners, in conjunction with asset custodians, are responsible for creating, implementing and updated operational procedures to comply with WISP requirements.

DEVCARE users are required to protect and ensure the Confidentiality, Integrity, Availability and Safety (CIAS) of data and systems, regardless of how its data is created, distributed or stored.

Security controls will be tailored accordingly so that cost-effective controls can be applied commensurate with the risk and sensitivity of the data and system; and

Security controls must be designed and maintained to ensure compliance with all legal requirements.

Violations

Any DEVCARE user found to have violated any policy, standard or procedure may be subject to disciplinary action, up to and including termination of employment. Violators of local, state, Federal, and/or international law may be reported to the appropriate law enforcement agency for civil and/or criminal prosecution.

Exceptions

While every exception to a standard potentially weakens protection mechanisms for DEVCARE systems and underlying data, occasionally exceptions will exist. When requesting an exception, users are required to submit a business justification for deviation from the standard in question.

Updates

Updates to the Written Information Security Program (WISP) will be announced to employees via management updates or email announcements. Changes will be noted in the Record of Changes to highlight the pertinent changes from the previous policies, procedures, standards and guidelines.

Key Terminology

In the realm of cybersecurity terminology, key terminology to be aware of includes:

Adequate Security. A term describing protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

Asset: A term describing any data, device, application, service or other component of the environment that supports information-related activities. An asset is a resource with economic value that a DEVCARE owns or controls.

Asset Custodian: A term describing a person or entity with the responsibility to assure that the assets are properly maintained, are used for the purposes intended, and that information regarding the equipment is properly documented.

Cardholder Data Environment (CDE): A term describing the area of the network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission. Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment and thus the scope of the PCI assessment

Cloud Computing. A term describing a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. It also includes commercial offerings for software-as-a-service, infrastructure-as-a-service, and platform-as-a-service.

Control: A term describing any management, operational, or technical method that is used to manage risk. Controls are designed to monitor and measure specific aspects of standards to help DEVCARE accomplish stated goals or objectives. All controls map to standards, but not all standards map to Controls.

Control Objective: A term describing targets or desired conditions to be met that are designed to ensure that policy intent is met. Where applicable, Control Objectives are directly linked to an industry-recognized leading practice to align DEVCARE with accepted due care requirements.

Data: A term describing an information resource that is maintained in electronic or digital format. Data may be accessed, searched, or retrieved via electronic networks or other electronic data processing technologies. Annex 1 (Data Classification & Handling Guidelines) provides guidance on data classification and handling restrictions.

Data/Process Owner: A term describing a person or entity that has been given formal responsibility for the security of an asset, asset category, process or the data hosted on the asset or process. It does not mean that the asset belongs to the owner in a legal sense. Data/process owners are formally responsible for making sure that assets are secure while they are being developed, produced, maintained, and used.

Encryption: A term describing the conversion of data from its original form to a form that can only be read by someone that can reverse the encryption process. The purpose of encryption is to prevent unauthorized disclosure of data.

Guidelines: A term describing recommended practices that are based on industry-recognized leading practices. Unlike Standards, Guidelines allow users to apply discretion or leeway in their interpretation, implementation, or use.

Information Security: A term that covers the protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. The focus is on the Confidentiality, Integrity, Availability and Safety (CIAS) of data.

THIS PART OF THE PAGE IS LEFT BLANK INTENTIONALLY

Information Security Program Structure

Management Direction for Information Security

The objective is to provide management direction and support for cybersecurity in accordance with business requirements and relevant laws and regulations. [6]

An Information Security Management System (ISMS) focuses on cybersecurity management and technology-related risks. The governing principle behind DEVCARE's ISMS is that, as with all management processes, the ISMS must remain effective and efficient in the long-term, adapting to changes in the internal organization and external environment.

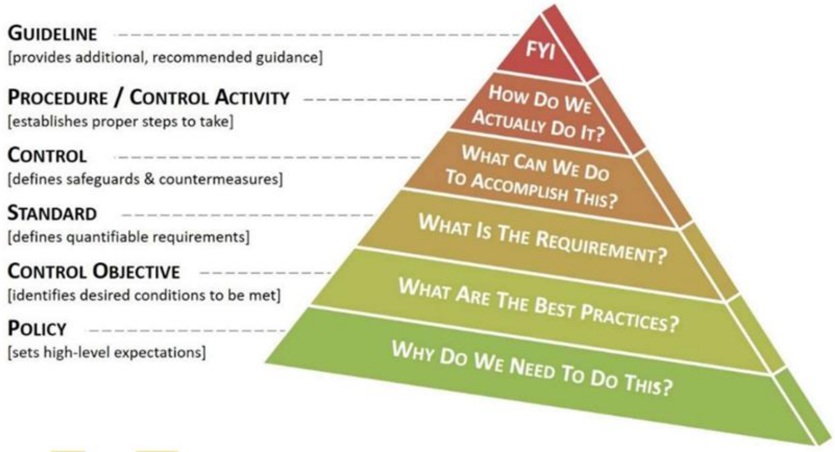
In accordance with leading practices, DEVCARE's ISMS incorporates the typical "Plan-Do-Check-Act" (PDCA), or Deming Cycle, approach:

Plan: This phase involves designing the ISMS, assessing IT-related risks, and selecting appropriate controls.
Do: This phase involves implementing and operating the appropriate security controls.
Check: This phase involves reviewing and evaluating the performance (efficiency and effectiveness) of the ISMS.
Act: This involves making changes, where necessary, to bring the ISMS back to optimal performance.

Policies, Standards, Procedures & Guidelines Structure

Cybersecurity documentation is comprised of six (6) main parts:

(1) Core policy that establishes management's intent.
(2) Control objective that identifies leading practices.
(3) Standards that provides quantifiable requirements.
(4) Controls identify desired conditions that are expected to be met.
(5) Procedures / Control Activities establish how tasks are performed to meet the requirements established in standards and to meet controls; and
(6) Guidelines are recommended, but not mandatory.


GUIDELINE
[provides additional, recommended guidance]
PROCEDURE / CONTROL ACTIVITY
[establishes proper steps to take]
CONTROL
[defines safeguards & countermeasures]
STANDARD
[defines quantifiable requirements]
CONTROL OBJECTIVE
[identifies desired conditions to be met]
POLICY
[sets high-level expectations]
FYI
HOW DO WE ACTUALLY DO IT?
WHAT CAN WE DO TO ACCOMPLISH THIS?
WHAT IS THE REQUIREMENT?
WHAT ARE THE BEST PRACTICES?
WHY DO WE NEED TO DO THIS?

Security, Privacy & Governance (GOV)

Management Intent: The purpose of the Security & Privacy Governance (GOV) policy is to specify the development, proactive management and ongoing review of DEVCARE's security and privacy program.

Policy: DEVCARE shall protect the confidentiality, integrity, availability and safety of its data and systems, regardless of how its data is created, distributed or stored. Security controls will be tailored accordingly so that cost-effective controls can be applied commensurate with the risk and sensitivity of the data and system, in accordance with all statutory, regulatory and contractual obligations.

Supporting Documentation: This policy is supported by the following control objectives, standards and guidelines.

GOV-1: Publishing Security & Privacy Policies

Control Objective: The organization establishes, publishes, maintains and disseminates security and privacy policies. [7]

Standard: DEVCARE's security and privacy policies and standards shall be represented in a consolidated document, the Written Information Security Program (WISP) that shall be:

(a) Endorsed by executive management; and
(b) Disseminated to the appropriate parties to ensure all DEVCARE personnel understand their applicable requirements.

Guidelines: An organization's cybersecurity policies create the roadmap for implementing cybersecurity and privacy measures to protect its most valuable assets. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it.

GOV-2: Assigned Security Responsibilities

Control Objective: The organization appoints an individual assigned with the mission and resources to centrally manage coordinate, develop, implement and maintain an organization-wide security program.[8]

Standard: Executive and line management shall take formal action to support cybersecurity through clearly-documented direction and commitment and shall ensure the action has been assigned. The overall authority and responsibility for managing the security program are delegated to DEVCARE's Chief Information Security Officer (CISO) and he / she is required to perform or delegate the following security management responsibilities:

(a) Establish, document and distribute security policies and procedures;
(b) Monitor and analyze security alerts and information;
(c) Distribute and escalate security alerts to appropriate personnel;
(d) Establish, document and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations;
(e) Administer user accounts, including additions, deletions and modifications; and
(f) Monitor and control all access to data.

Guidelines: Central management refers to the organization-wide management and implementation of selected cybersecurity controls and related processes. Central management includes planning, implementing, assessing, authorizing and monitoring the organization-defined, centrally managed security controls and processes. Centrally-managed security controls and processes may also meet independence requirements for assessments in support of initial and ongoing authorizations to operate as part of organizational continuous monitoring.

THIS PART OF THE PAGE IS LEFT BLANK INTENTIONALLY

Endpoint Security (END)

Management Intent: The purpose of the Endpoint Security (END) policy is to ensure that endpoint devices are appropriately protected from reasonable threats to the confidentiality, integrity, availability and safety of the device and its data. Applicable statutory, regulatory and contractual compliance obligations dictate the safeguards that must be in place to protect the confidentiality, integrity, availability and safety considerations.

Policy: DEVCARE shall implement the concept of "least functionality" for its technology endpoints and proactively govern security mechanisms to keep its technology assets secure from evolving threats.

Supporting Documentation: This policy is supported by the following control objectives, standards and guidelines.

END-1: Malicious Code Protection (Anti-Malware)

Control Objective: The organization: [38]

Employs malicious code protection mechanisms at system entry and exit points and at workstations, servers or mobile computing devices on the network to detect and eradicate malicious code:

- o Transported by electronic mail, electronic mail attachments, web accesses, removable media or other common means; or
- o Inserted through the exploitation of system vulnerabilities;

Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures;

Configures malicious code protection mechanisms to:

- o Perform periodic scans of the system and real-time scans of files from external sources as the files are downloaded, opened or executed in accordance with organizational security policy;
- o Quarantines malicious code; send alert to an administrator; in response to malicious code detection; and Addresses the receipt of false positives during malicious code detection.

Standard: Asset custodians are required to:

(a) Deploy the DEVCARE-approved anti-malware software on all systems capable of running anti-malware software, including, but not limited to:

1. Workstations;
2. Servers;
3. Tablets;
4. Mobile phones;

(b) Ensure that the DEVCARE-approved anti-malware software is capable of detecting, removing and protecting against all known types of malware; and

(c) Perform periodic evaluations to identify and evaluate evolving malware threats on systems considered to be not commonly affected by malware, in order to confirm whether such systems continue to not require anti-malware software.

Guidelines: Systems not capable of running anti-malware software should have a documented business justification as to why anti-malware software cannot be run and what compensating controls are in place to minimize the risk associated with the lack of anti-malware software on that system.

END-2: File Integrity Monitoring (FIM)

Control Objective: Systems detect and report unauthorized changes to system files and configurations.

Standard: On critical systems, asset custodians are required to:

(a) Deploy File Integrity Monitoring (FIM) tools to alert personnel to unauthorized modification of critical system files, configuration files or content files; and configure the software to perform critical file comparisons at least weekly;

(b) Verify the use of FIM tools by observing system settings and monitored files, as well as reviewing results from monitoring activities. Examples of files that should be monitored:

1. System executables;
2. Application executables;
3. Configuration and parameter files; and
4. Centrally stored, historical or archived, log and audit files.

(c) Verify the tools are configured to alert personnel to unauthorized modification of critical files and to perform critical file comparisons at least weekly.

Guidelines: FIM tools should be used to ensure that critical system files (including sensitive system and application executables, libraries and configurations) have not been altered. The reporting system should have the ability to account for routine and expected changes; highlight and alert on unusual or unexpected alterations; show the history of configuration changes over time and identify who made the change (including the original logged-in account in the event of a user ID switch, such as with the su or sudo command).

These integrity checks should identify suspicious system alterations such as: owner and permissions changes to files or directories; the use of alternate data streams which could be used to hide malicious activities; and the introduction of extra files into key system areas (which could indicate malicious payloads left by attackers or additional files inappropriately added during batch distribution processes).

END-3: Mobile Code

Control Objective: The organization addresses operating system-independent applications. The organization:

Defines acceptable and unacceptable mobile code and mobile code technologies;

Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and Authorizes, monitors and controls the use of mobile code within systems.

Standard: Asset custodians and data / process owners are required to manage the use of mobile code technologies through:

(a) Managing operating system-independent applications, based on the threat posed since operating system-independent applications are applications that can run on multiple operating systems; and
   1. Defining acceptable and unacceptable mobile code and mobile code technologies;
   2. Establishing usage restrictions for mobile code and mobile code technologies; and

(b) Developing secure system configurations to address mobile code usage within systems that include, but is not limited to:
   1. Preventing the download and execution of prohibited mobile code;
   2. Preventing the automatic execution of mobile code; and
   3. Uninstalling operating system-independent applications from systems where the applications are not required for a business purpose.

Guidelines: Operating system independent applications (e.g., Java, Flash, QuickTime, etc.) promote functionality across platforms, but are considered security risks. Operating system-independent applications are applications that can run on multiple operating systems. Such applications promote portability and reconstitution on different platform architectures, increasing the availability of critical functions within organizations while systems with specific operating systems are under attack.

Decisions regarding the employment of mobile code within DEVCARE's systems are based on the potential for the code to cause damage to the systems if used maliciously. Mobile code technologies include, for example, Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices (e.g., smartphones).

The following mobile code and mobile code technologies are defined below as High Risk, Moderate Risk and Low Risk:

High Risk: Mobile code technologies that exhibit functionality allowing unmediated access to host and remote services and resources.
Medium Risk: Mobile code technologies that have functionality allowing mediated or controlled access to local services and resources.
Low Risk: Mobile code technologies that have functionality with no capability for unmediated access to local services and resources.

Ensure usage restrictions and implementation guidelines for mobile code and mobile code technologies are limited to:

Identification & Authentication (IAC)

Management Intent: The purpose of the Identification & Authentication (IAC) policy is to implement the concept of "least privilege" through limiting access to DEVCARE's systems and data to authorized users only.

Policy: DEVCARE shall implement the principle of "least privilege" within logical access control mechanisms so that only authorized users can gain access to DEVCARE's systems and data.

Supporting Documentation: This policy is supported by the following control objectives, standards and guidelines.

IAC-1: User Provisioning & De-Provisioning

Control Objective: The organization implements a formal user registration and de-registration process to govern the assignment of access rights.

Standard: DEVCARE's Identity and Access Management (IAM) team shall implement and manage a formal user access provisioning process to assign and / or revoke access rights for all user types to all systems and services.

Guidelines: Provisioning user access (e.g., employees, contractors, customers (tenants), business partners, and / or supplier relationships) to data and organizationally owned or managed (physical and virtual) applications, infrastructure systems and network components shall be authorized by the organization's management prior to access being granted and appropriately restricted as per established policies and procedures. Upon request, the provider shall inform customer (tenant) of this user access, especially if customer (tenant) data is used as part the service and / or customer (tenant) has some shared responsibility for implementation of control.

Timely de-provisioning (revocation or modification) of user access to data and organizationally owned or managed (physical and virtual) applications, infrastructure systems and network components, shall be implemented as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change or transfer). Upon request, the provider shall inform customer (tenant) of these changes, especially if customer (tenant) data is used as part the service and / or customer (tenant) has some shared responsibility for implementation of control.

IAC-2: Account Management

Control Objective: The organization manages system accounts, including:

- Identifying account types (e.g., individual, group, system, application, guest / anonymous and temporary);
- Establishing conditions for group membership.

- Identifying authorized users of the system and specifying access privileges.
- Requiring appropriate approvals for requests to establish accounts.
- Establishing, activating, modifying, disabling and removing accounts;
- Specifically authorizing and monitoring the use of guest / anonymous and temporary accounts.
- Notifying account managers when temporary accounts are no longer required and when system users are terminated, transferred or system usage or need-to-know / need-to-share changes.
- Deactivating accounts that are no longer required.

- Granting access to the system based on a valid access authorization; and Reviewing accounts on a regular basis.

Standard: DEVCARE's IT department is responsible for ensuring proper user identification and authentication management for all standard and privileged users on all systems, as follows:

(a) Control addition, deletion and modification of user IDs, credentials and other identifier objects to ensure authorized use is maintained.
(b) Verify user identity before issuing initial passwords or performing password resets.
(c) Set passwords for first-time use and resets to a unique value for each user and change immediately after the first use.
(d) Immediately revoke access for any terminated users.

THIS PART OF THE PAGE IS LEFT BLANK INTENTIONALLY

Data Classification and Handling

Data Classification

Information assets are assigned a sensitivity level based on the appropriate audience for the information. If the information has been previously classified by regulatory, legal, contractual, or company directive, then that classification will take precedence. The sensitivity level then guides the selection of protective measures to secure the information. All data are to be assigned one of the following four sensitivity levels:

CLASSIFICATION		DESCRIPTION
RESTRICTED	Definition	Restricted information is highly valuable, highly sensitive business information and the level of protection is dictated externally by legal and/or contractual requirements. Restricted information must be limited to only authorized employees, contractors, and business partners with a specific business need.
	Potential Impact of Loss	SIGNIFICANT DAMAGE would occur if Restricted information were to become available to unauthorized parties either internal or external to DEVCARE. Impact could include negatively affecting DEVCARE's competitive position, violating regulatory requirements, damaging the company's reputation, violating contractual requirements, and posing an identity theft risk.
CONFIDENTIAL	Definition	Confidential information is highly valuable, sensitive business information and the level of protection is dictated internally by DEVCARE
	Potential Impact of Loss	MODERATE DAMAGE would occur if Confidential information were to become available to unauthorized parties either internal or external to DEVCARE. Impact could include negatively affecting DEVCARE's competitive position, damaging the company's reputation, violating contractual requirements, and exposing the geographic location of individuals.
INTERNAL USE	Definition	Internal Use information is information originated or owned by DEVCARE, or entrusted to it by others. Internal Use information may be shared with authorized employees, contractors, and business partners who have a business need, but may not be released to the general public, due to the negative impact it might have on the company's business interests.
	Potential Impact of Loss	MINIMAL or NO DAMAGE would occur if Internal Use information were to become available to unauthorized parties either internal or external to DEVCARE. Impact could include damaging the company's reputation and violating contractual requirements.

PUBLIC	Definition	Public information is information that has been approved for release to the general public and is freely shareable both internally and externally.
	Potential Impact of Loss	NO DAMAGE would occur if Public information were to become available to parties either internal or external to DEVCARE. Impact would not be damaging or a risk to business operations.

Labeling

Labeling is the practice of marking a system or document with its appropriate sensitivity level so that others know how to appropriately handle the information. There are several methods for labeling information assets.

Printed. Information that can be printed (e.g., spreadsheets, files, reports, drawings, or handouts) should contain one of the following confidentiality symbols in the document footer on every printed page (see below), or simply the words if the graphic is not technically feasible. The exception for labeling is with marketing material since marketing material is primarily developed for public release.

Displayed. Restricted or Confidential information that is displayed or viewed (e.g., websites, presentations, etc.) must be labeled with its classification as part of the display.

General Assumptions

- Any information created or received by DEVCARE employees in the performance of their jobs at is Internal Use, by default, unless the information requires greater confidentiality or is approved for release to the general public.
- Treat information that is not assigned a classification level as "Internal Use" at a minimum and use corresponding controls.
- When combining information with different sensitivity levels into a single application or database, assign the most restrictive classification of the combined asset. For example, if an application contains Internal Use and Confidential information, the entire application is Confidential.
- Restricted, Confidential and Internal Use information must never be released to the general public but may be shared with third parties, such as government agencies, business partners, or consultants, when there is a business need to do so, and the appropriate security controls are in place according to the level of classification.
- You may not change the format or media of information if the new format or media you will be using does not have the same level of security controls in place. For example, you may not export Restricted information from a secured database to an unprotected Microsoft Excel spreadsheet.

Personal Data (PD)

PD is any information about an individual maintained by DEVCARE including any information that:

Can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and

Is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Sensitive PD (sPD) is always PD, but PD is not always sPD. Examples of PD include, but are not limited to:

Name

- o Full name;
- o Maiden name;
- o Mother's maiden name; and
- o Alias(es);

Personal Identification Numbers

- o Social Security Number (SSN);
- o Passport number;
- o Driver's license number;
- o Taxpayer Identification Number (TIN), and
- o Financial account or

credit card number; Address
Information

- o Home address; and
- o Personal email address;

Personal Characteristics

- o Photographic image (especially of the face or other identifying characteristics, such as scars or tattoos);
- o Fingerprints;
- o Handwriting, and

THIS PART OF THE PAGE IS LEFT BLANK INTENTIONALLY

Data Handling Guidelines

Handling Controls	Restricted	Confidential	Internal Use	Public
Non-Disclosure Agreement (NDA)	NDA is required prior to access by non-DEVCARE employees.	NDA is recommended prior to access by non-DEVCARE employees.	No NDA Requirements	No NDA Requirements
Internal Network Transmission (wired & wireless)	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited	▪ Encryption is recommended ▪ Instant Messaging is prohibited ▪ FTP is prohibited	No requirements	No Requirements
External Network Transmission (wired & wireless)	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited ▪ Remote access should be used only when necessary and only with VPN and two-factor authentication	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited	▪ Encryption is recommended ▪ Instant Messaging is prohibited ▪ FTP is prohibited	No Requirements
Data At Rest (file servers, databases, archives, etc.)	▪ Encryption is required ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific individuals	▪ Encryption is recommended ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups	▪ Encryption is recommended ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups	▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups
Mobile Devices (iPhone, iPad, MP3 player, USB drive, etc.)	▪ Encryption is required ▪ Remote wipe must be enabled, if possible	▪ Encryption is required ▪ Remote wipe must be enabled, if possible	▪ Encryption is recommended ▪ Remote wipe must be enabled, if possible	No Special Requirements
Email (with and without attachments)	▪ Encryption is required ▪ Do not forward attachments)	▪ Encryption is required ▪ Do not forward attachments)	Encryption is recommended	No special requirements
Physical Mail	▪ Mark “Open by Addressee Only” ▪ Use “Certified Mail” and sealed, tamper-resistant	▪ Mark “Open by Addressee Only” ▪ Use “Certified Mail” and sealed, tamper-resistant	▪ Mail with company interoffice mail ▪ US Mail or other public delivery	No Requirements

	envelopes for external mailings ▪ Delivery confirmation is required ▪ Hand deliver internally	envelopes for external mailings ▪ Delivery confirmation is required ▪ Hand delivery is recommended	systems and sealed, tamper-resistant envelopes for external mailings	
Printer	▪ Verify destination printer ▪ Attend printer while printing	▪ Verify destination printer ▪ Attend printer while printing	▪ Verify destination printer ▪ Retrieve printed material without delay	No Requirements

Data Retention Periods

The following schedule highlights suggested retention periods* for some of the major categories of data:

* Retention periods are measured in years, after the event occurrence (e.g., termination, expiration, contract, filing, etc.)

CATEGORY	TYPE OF RECORD	RETENTION PERIOD
Business Records	Amendments	Permanent
	Annual Reports	Permanent
	Articles of Incorporation	Permanent
	Board of Directors (elections, minutes, committees, etc.)	Permanent
	Bylaws	Permanent
	Capital stock & bond records	Permanent
	Charter	Permanent
	Contracts & agreements	Permanent
	Copyrights	Permanent
	Correspondence (General)	5
	Correspondence (Legal)	Permanent
	Partnership agreement	Permanent
	Patents	Permanent
	Service marks	Permanent
	Stock transfers	Permanent
	Trademarks	Permanent
Financial Records	Audit report (external)	Permanent
	Audit report (internal)	3
	Balance sheets	Permanent
	Bank deposit slips, reconciliations & statements	7
	Bills of lading	3
	Budgets	3
	Cash disbursement & receipt record	7

	Checks (canceled)	3
	Credit memos	3
	Depreciation schedule	7
	Dividend register & canceled dividend checks	Permanent
	Employee expense reports	3
	Employee payroll records (W-2, W-4, annual earnings records, etc.)	7
	Financial statements (annual)	Permanent
	Freight bills	3
	General ledger	Permanent
	Internal reports (work orders, sales reports, production reports)	3
	Inventory lists	3
	Investments (sales & purchases)	Permanent
	Profit / Loss statements	Permanent
	Purchase and sales contracts	3
	Purchase order	3
	Subsidiary ledgers (accounts receivable, accounts payable, etc.)	Permanent
	Tax returns	Permanent
	Vendor Invoices	7
	Worthless securities	7

THIS PART OF THE PAGE IS LEFT BLANK INTENTIONALLY

Baseline Security Categorization Guidelines

Assets and services are categorized by two primary attributes: (a) the potential impact they pose from misuse and (b) the data classification level of the data processed, stored or transmitted by the asset or process. These two attributes combine to establish a basis for controls that should be assigned to that system or asset. This basis is called an Assurance Level (AL).

Data Sensitivity

This is straightforward where the data sensitivity rating represents the highest data classification of the data processed, stored or transmitted by the asset or process

Safety & Criticality

The Safety & Criticality (SC) rating reflects two aspects of the "importance" of the asset or process:

> On one hand, SC simply represents the importance of the asset relative to the achievement of the company's goals and objectives (e.g., business critical, mission critical, or non-critical). On the other hand, SC represents the potential for harm that misuse of the asset or service could cause to DEVCARE, its clients, its partners, or the general public.

The three (3) SC ratings are:

SC-1: Mission Critical. This category involves systems, services and data that is determined to be vital to the operations or mission effectiveness of DEVCARE:

- Includes systems, services or data with the potential to significantly impact the brand, revenue or customers.
- Any business interruption would have a significant impact on DEVCARE's mission.
- Cannot go down without having a significant impact on DEVCARE's mission.

The consequences of loss of integrity or availability of a SC-1 system are unacceptable and could include the immediate and sustained loss of mission effectiveness.

- Requires the most stringent protection measures that exceed leading practices to ensure adequate security.
-
- Safety aspects of SC-1 systems, services and data could lead to: Catastrophic hardware failure; Unauthorized physical access to premises; and/or Physical injury to users.

SC-2: Business Critical. This category involves systems, services and data that are determined to be important to the support of DEVCARE's business operations:

- Includes systems, services or data with the potential to moderately impact the brand, revenue or customers.
- Affected systems, services or data can go down for up to twenty-four (24) hours (e.g., one (1) business day) without having a significant impact on DEVCARE's mission.

  Loss of availability is difficult to deal with and can only be tolerated for a short time.

    - The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or the ability to operate.

- The consequences of loss of integrity are unacceptable.

- <u>Requires protection measures equal to or beyond leading practices</u> to ensure adequate security.
- Safety aspects of SC-2 systems could lead to: Loss of privacy; and/or Unwanted harassment

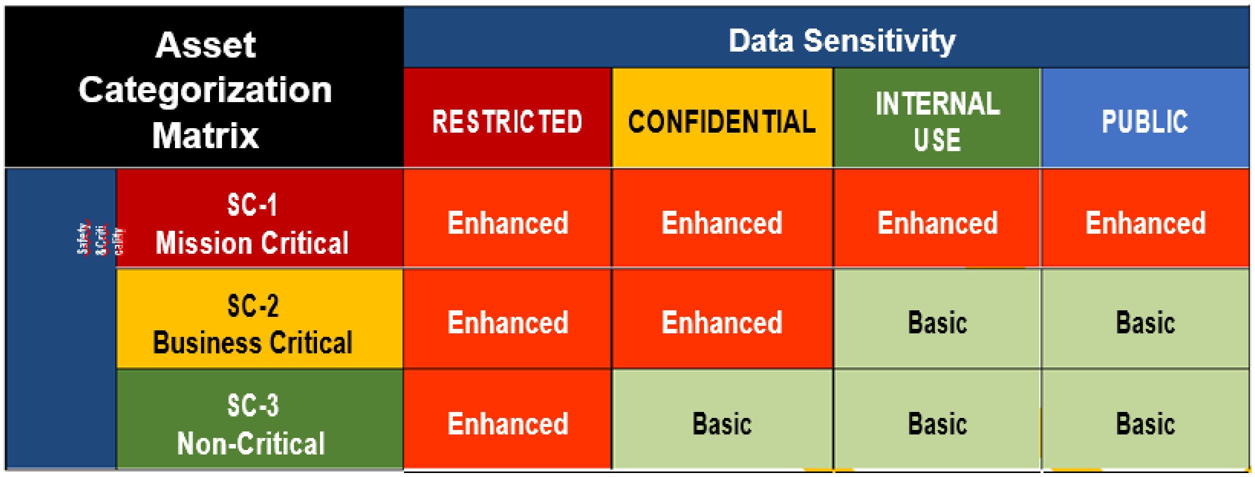
<u>SC-3: Non-Critical</u>. This category involves systems, services and data that are necessary for the conduct of day-to-day operations, but are not business critical in the short-term:

- Includes systems, services or data with little or potential to impact the brand, revenue or customers.
- Affected systems, services or data can go down for up to seventy-two (72) hours (e.g., three (3) business days) without having a significant impact on DEVCARE's mission.

  The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness.

  The consequences could include the delay or degradation of services or routine activities.
- <u>Requires protection measures that are commensurate with leading practices</u> to ensure adequate security.
- Safety aspects of SC-3 systems could lead to: Inconvenience, Frustration, and/or Embarrassment.

Where the data sensitivity and SC levels meet are considered the Assurance Levels (AL). The AL represents the "level of effort" that is needed to properly ensure the Confidentiality, Integrity, Availability and Safety (CIAS) of the asset or process.



Asset Categorization Matrix		Data Sensitivity			
		RESTRICTED	CONFIDENTIAL	INTERNAL USE	PUBLIC
Safety &Criticality	SC-1 Mission Critical	Enhanced	Enhanced	Enhanced	Enhanced
	SC-2 Business Critical	Enhanced	Enhanced	Basic	Basic
	SC-3 Non-Critical	Enhanced	Basic	Basic	Basic

Basic Assurance Requirements

The minimum level of controls is defined as industry-recognized leading practices (e.g., PCI DSS, NIST 800-53, ISO 27002, etc.).

For security controls in Basic assurance projects or initiatives, the focus is on the digital security controls being in place with the expectation that no obvious errors exist and that as flaws are discovered they are addressed in a timely manner.

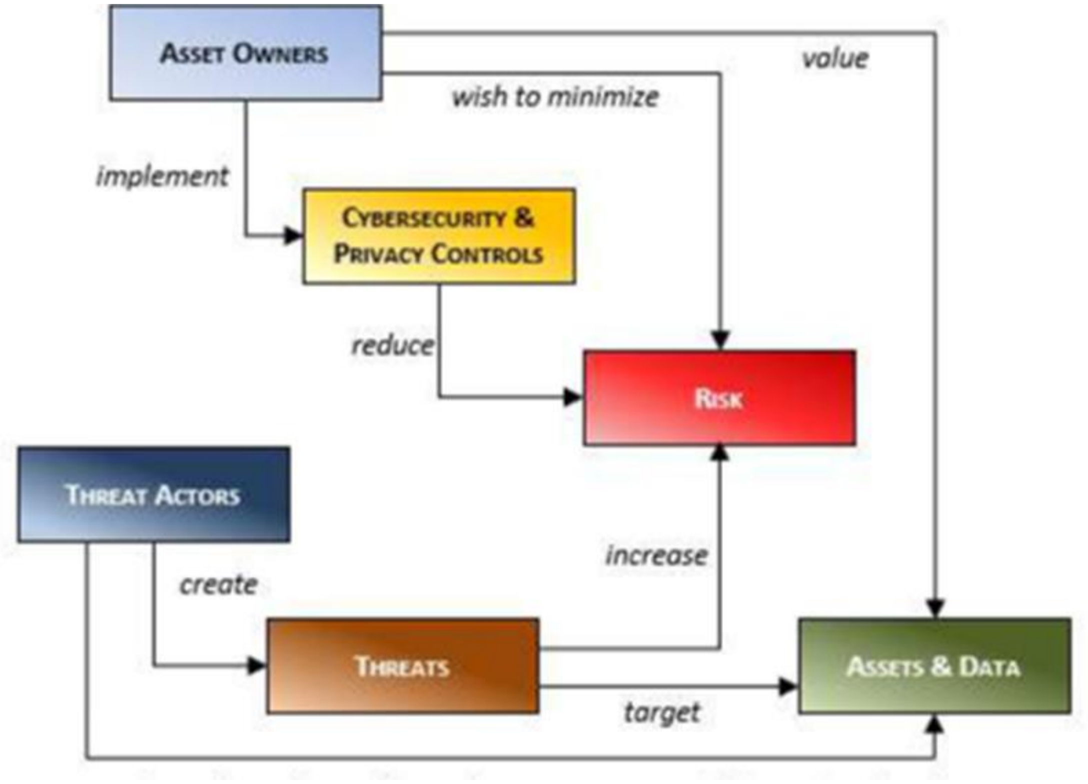
THIS PART OF THE PAGE IS LEFT BLANK INTENTIONALLY

Risk Management Framework (RMF)

DEVCARE maintains a cybersecurity risk management program to evaluate threats and vulnerabilities in order to assure the creation of appropriate remediation plans.

Risk Management Overview

There is sometimes conflict between cybersecurity and other general system/software engineering principles. Cybersecurity can sometimes be construed as interfering with ``ease of use'' where installing security countermeasures take more effort than a ``trivial'' installation that works, but is insecure. Often, this apparent conflict can be resolved by re-thinking the problem and it is generally possible to make a secure system also easy to use. Based on the value owners place on their assets, it is a necessity to impose countermeasures to mitigate any risks posed by specific threats.



Risk Management Framework (RMF)

Risk management requires finding security equilibrium between vulnerabilities and acceptable security controls. This equilibrium can be thought of as acceptable risk – it changes as vulnerabilities and controls change. From a systems perspective, the components used to determine acceptable risk cover the entire Defense-in-Depth (DiD) breadth. If one component is weakened, another component must be strengthened to maintain the same level of security assurance. Risk management activities can be applied to both new and legacy systems.

Incident Response Plan (IRP)

By the very nature of every incident being somewhat different, the guidelines provided in this Incident Response Plan (IRP) do not comprise an exhaustive set of incident handling procedures. These guidelines document basic information about responding to incidents that can be used regardless of hardware platform or operating system. This plan describes the stages of incident identification and handling, with the focus on preparation and follow-up, including reporting guidelines and requirements.

Plan Objectives

The objective of Incident Response Plan (IRP) is to:

- Limit immediate incident impact to customers and business partners.
- Recover from the incident.
- Determine how the incident occurred.
- Find out how to avoid further exploitation of the same vulnerability.
- Avoid escalation and further incidents.
- Assess the impact and damage in terms of financial impact and loss of image.
- Update company policies, procedures, standards and guidelines as needed.
- Determine who initiated the incident for possible criminal and/or civil prosecution.

Incident Discovery

Malicious Activity	Possible Action of Incident
Denial of Service (DoS) Examples	**You might be experiencing a DoS if you see…**
Network-based DoS against a particular host	• User reports of system unavailability
	• Unexplained connection losses
	• Network intrusion detection alerts
	• Host intrusion detection alerts (until the host is overwhelmed)
	• Increased network bandwidth utilization
	• Large number of connections to a single host
	• Asymmetric network traffic pattern (large amount of traffic going to the host, little traffic coming
	from the host)
	• Firewall and router log entries
	• Packets with unusual source addresses
Network-based DoS against a network	• User reports of system and network unavailability
	• Unexplained connection losses
	• Network intrusion detection alerts
	• Increased network bandwidth utilization

	• Asymmetric network traffic pattern (large amount of traffic entering the network, little traffic leaving
	the network)
	• Firewall and router log entries
	• Packets with unusual source addresses
	• Packets with nonexistent destination addresses
DoS against the operating system of a host	• User reports of system and application unavailability
	• Network and host intrusion detection alerts
	• Operating system log entries
	• Packets with unusual source addresses
DoS against an application on a host	• User reports of application unavailability
	• Network and host intrusion detection alerts
	• Application log entries
	• Packets with unusual source addresses

THIS PART OF THE PAGE IS LEFT BLANK INTENTIONALLY

Disaster Recovery Plan (DRP) & Business Continuity Plan (BCP)

Disaster Recovery Plan (DRP)

A Disaster Recovery Plan (DRP) specifies emergency response procedures, including specifying individual responsibility for responding to emergency situations and specifying procedures to enable team members to communicate with each other and with management during and after an emergency.

DRP Scoping Requirements

The DRP requirements for critical assets are summarized below:

Disaster Recovery Plan (DRP) Summary				
Criticality		MAC-I	MAC-II	MAC-III
Data Sensitivity	Restricted	High security required; must be in Disaster Recovery Plan	High security required; must be in Disaster Recovery Plan	High security required; must be in Disaster Recovery Plan
	Confidential	Moderate security required; must be in Disaster Recovery Plan	Moderate security required; may be in Disaster Recovery Plan	Moderate security required; need not be in Disaster Recovery Plan
	Internal User	Minimal security required; must be in Disaster Recovery Plan	Minimal security required; may be in Disaster Recovery Plan	Minimal security required; need not be in Disaster Recovery Plan
	Public	Minimal security required; must be in Disaster Recovery Plan	Minimal security required; may be in Disaster Recovery Plan	Minimal Security, need not be in Disaster

Backup copies of data and software that are sufficient for recovery from an emergency situation pertaining to critical assets must be stored at a secure, external site providing standard protection against hazards such as fire, flood, earthquake, theft, and decay. Requirements and procedures for such offsite backup shall be included in the DRP, including procedures and authorities for obtaining access to such sites in the event of an emergency.

Disaster recovery requirements should be specified when establishing maintenance agreements with vendors supplying components of critical resources. Ensure that vendors can provide replacement components within a reasonable period of time when planning system upgrades or deployments.

Data Backup Availability

Backup copies of data and software must be sufficient to satisfy DRP requirements, application or other critical information asset processing requirements, and any functional requirements of any critical information asset custodian dependent upon such data. Backup copies for disaster recovery purposes must be stored at a secure, off-site location that provides industry-standard protection. These backup requirements extend to all information systems and data necessary to be reconstituted in the event of a disaster.

THIS PART OF THE PAGE IS LEFT BLANK INTENTIONALLY