**Table of Contents**

1.0 Purpose

2.0 Scope & Definitions

3.0 Roles & Responsibilities

4.0 Policy Statements

5.0 Compliance/Exceptions/Enforcement

6.0 Review Cycle

7.0 References

8.0 Document Version History

**1.0 Purpose**

The purpose of the policy is to establish an effective and consistent approach and framework for information security incident handling processes and procedures that are integrated into daily IT operations. Information security incident handling covers all aspects of responding to information security incidents affecting, at a minimum, availability, integrity, and confidentiality of Costco Wholesale (Costco) networks, systems, applications, data, and other information assets. Incident handling includes communication on security events and weaknesses, gathering and communicating information for required regulatory disclosures, conducting analysis and investigation of the incident as needed, restoring normal business operations affected by information security incidents as soon as possible, and minimizing negative impacts of information security incidents. Refer to the Information Security Incident Response Management Standard and related documents for more detailed requirements pertaining to the incident response process.

# Scope & Definitions

The scope of this policy includes all Costco-managed assets, information resources and internal users. This policy applies to all Costco’s external users accessing Costco data and assets, including vendors, suppliers and other third parties engaged to perform business with Costco; however, these parties’ information security incident response capabilities and obligations shall be evaluated in accordance with the Information Security Third Party Risk Management Policy and are out of scope of this policy. Third parties’ information security incident handling, reporting, and collaboration obligations shall be legally binding and properly outlined in contract agreements between Costco and other parties.

This policy applies to all Costco information systems and data asset users, including but not limited to: employees, vendors, consultants, 3rd party contractors and agents.

Costco Information Security (IS) policies and standards are in effect for all countries unless they are superseded by specific in-country legal and policy requirements due to location regulations/circumstances. These exceptions, written and maintained in-country, will be reviewed centrally for appropriateness before adoption. The following take precedence over the policies and standards:

* + - Regulatory and legal statutes, laws, contractual agreements, and prescriptive and obligatory requirements
    - IS policies and standards explicitly approved and adopted by in-country IS teams. Such policies and standards must clearly delineate functional responsibilities

For the purpose of this policy and related documents, an “**information security event**” is defined as an unauthorized occurrence of a Costco data, device, system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be information security relevant.

An “**information security incident**” is defined as a single or a series of unwanted or unexpected information security events that have a significant probability of compromising the confidentiality, integrity, and /or availability of Costco information assets, business operations, and information security.

“**Personal Data**” is information relating to an identified or identifiable natural person.

A “**Personal Data Incident**” is an information security incident that could materially compromise the privacy, confidentiality, security or integrity of Personal Data, including any unauthorized disclosure of or access to Personal Data, loss or alteration of Personal Data, or unauthorized use or manipulation of Personal Data. To the extent that an information security incident involves *Restricted, Regulated, or Confidential* data, applicable law may define what constitutes a data security breach and how it is to be managed.

# 3.0 Roles & Responsibilities

**Information Security Vice President:** accountable for the development, implementation, and governance of Information Security strategy as well as setting of information security objectives related to information security incident response management. Has the authority and accountability to ensure that Information Security policies and standards are enacted and enforced.

**Information Security Vice President and Directors:** responsible for developing and maintaining the Costco Information Security incident response management program, management of information security objectives related to incident response management, and maintenance of Information Security policies and standards.

**HIPAA (Health Insurance Portability and Accountability Act of 1996) Security Officer:** accountable for implementation of incident response management processes for security events and incidents affecting asset storage and processing of electronic Protected Health Information (ePHI).

**All employees and contractors:** It is the duty of all Costco staff to report immediately any suspected or confirmed Personal Data Incident by reporting the incident as soon as possible.

# Policy Statements

## Incident Management Process Lifecycle

An information security incident response management lifecycle process shall be established by the Information Security department and will contain the following phases, at a minimum:

* + 1. Pre-event -- preparation and testing
    2. Detection -- identification and reporting of event
    3. Assessment -- analysis of event
    4. Activation -- Working group response to incident; resolution, record and recovery
    5. Post-incident -- review and lessons learned

If technically and operationally feasible, information security event and incident reporting, tracking and documentation shall be supported by an automated application and a database used to record reported vulnerability, event, and/or incident information.

## Information Security Incident Working Group

An Information Security Incident Working Group (“Working Group”) shall be established to prepare for and respond to Incidents; mitigate harm; minimize reputational, commercial, and legal risk; satisfy Costco’s legal obligations, including those to members and affiliates; and defray or recover costs resulting from an information security incident. The core members of the Working Group (collectively, the “Core Working Group”) are:

1. The Legal Incident Response Manager;
2. The Information Security Incident Response Manager; and
3. A Risk Management representative.

The Core Working Group shall coordinate their activities with key representatives of other departments and functions within Costco (such as Treasury, Membership, Human Resources, International, Loss Prevention, and Operations) as needed. Thus, except for the Core Working Group, the Working Group for each Personal Data Incident will comprise different members, depending on the type and scope of each such incident.

The Core Working Group is responsible for developing the standards, plans and guidelines to manage each phase of an information security incident, as identified above. The Legal Incident Response Manager and the Information Security Incident Response Manager shall be jointly responsible for maintaining the Costco Data Security Incident Response Plan. This plan shall define Costco’s step-by-step process and procedures for responding to a data security breach, including notification requirements and procedures. At a minimum, an information security incident affecting *Restricted, Regulated,* and *Confidential* data shall be responded to and managed in accordance with the plan, including incidents involving Personal Data that may require notification to authorities or individuals.

## Technical Incident Response Team

The Information Security department shall be responsible for establishing, supporting, and maintaining a technical incident response team. This team shall be managed by the Information Security Incident Response Manager. The technical incident response team shall be responsible for responding to information security incidents throughout the Costco-managed environment, including incident verification and declaration, incident analysis, response, and resolution and incident documentation.

The technical incident response team shall coordinate its activities with the Core Working Group, Working Group, and other departments and functions within Costco as needed. The key representatives of these other departments and functions within Costco shall provide all requested assistance to the technical incident response team in a timely manner.

## Investigative Support and Forensics

Forensics requirements shall be considered when conducting incident analysis and performing response and resolution activities in order not to violate the chain-of-custody principle. Process shall be established and followed if investigative support from law enforcement agency is required as determined by the Core Working Group.

# 5.0 Compliance/Exceptions/Enforcement

Compliance is expected within 90 days of standard approval. If a portion of the standard cannot be followed, an exception must be requested and approved via the Risk Acceptance Process. Failure to comply with this standard will result in management intervention and may result in disciplinary action. This standard will remain enforceable until modified and approved, or retired and removed from active publication.

Report violations or suspected violations via email to [infosecpolicyteam@costco.com](mailto:infosecpolicyteam@costco.com) immediately.

# 6.0 Review Cycle

This standard will be reviewed based on the criteria defined in the Information Security Policy Management Standard.

Questions or concerns should be directed to [infosecpolicyteam@costco.com](mailto:infosecpolicyteam@costco.com)

# 7.0 References

Information Security Third Party Risk Management Policy Information Security Incident Response Management Standard Costco Data Security Incident Response Plan

# 8.0 Document Review History

|  |  |  |  |
| --- | --- | --- | --- |
| **Review #** | **Comments** | **Date** | **Executive Approver** |
| 1.0 |  | 9/28/2007 | IS Council |
| 1.2 |  | 6/24/2009 | Mark Mattis |
| 1.3 |  | 12/28/10 | Mark Mattis |
| 1.4 |  | 12/17/13 | Franklin Donahoe |
| 2.0 | Policy revised and updates to the content made | 12/19/16 | Tim Bowersock |
| 3.0 | 2.0 Scope language updated to reflect global scope of policy  6.0 Review Cycle - updated standardized language added  GDPR content adds/edits by Legal:  1.0 Incident handling expanded  2.0 Definition of security event and Scope language updated  4.0 Legal department GDPR compatible language added |  | Tim Bowersock |
| 4.0 | Annual Review | 2/14/19 | Tim Bowersock |
| 4.1 | Annual Review  Signature block: Director signature removed per IS Policy Management Standard  Section 2.0 update:   * Added “& Definitions” * Paragraph restructure * Updated last paragraph to present requirements   Swapped sections 5.0 & 7.0 to meet updated document format requirements. | 12/11/2019 | Tim Bowersock |