Information Security Policy

Policy #	TBI-ISP-001	Effective Date	7-March-25	Email	Cybersecurity@trueblue.com
Version	1.9	Owner	GRC/Information Security		

Contents

1) Purpose

Information, in any of its forms, and its supporting processes, systems and networks are the most critical business assets on which TrueBlue, Inc. (TBI or TrueBlue) business resiliency and growth depend. As such, they must be adequately and actively protected from a variety of threats to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities. This Information Security Policy is designed to provide the Information Security guidelines to which all TBI employees, contractors and vendors must adhere.

Effective Information Security is a team effort involving the participation and support of every TBI employee, contractor, or vendor who deals with information and/or information systems. It is the responsibility of every user to know these guidelines, and to conduct their activities accordingly.

2) Scope

This Policy applies to all TrueBlue employees, and non-employees including all personnel affiliated with third parties that have access to TBI systems, networks and assets, and data. This policy also applies to all equipment that is owned or leased by TBI.

This policy applies to the information, electronic and computing devices, and network resources and services used to conduct TBI business or interact with any business systems and data, whether owned or leased by TBI, an employee, or a third party.

3) Glossary

Employee – Any individual employed by TrueBlue or any of its subsidiaries.

Non-Employee - Any individual employed by a third-party for the purpose of providing services to TrueBlue or any of its subsidiaries.

TBI Assets – includes any TBI owned system or device that stores TBI information/data including in on-prem or on-cloud platforms. Also, any TBI information/data stored on non-TBI owned systems.

Users – Employees and Non-Employees that interact with TBI Assets, data or network to conduct TBI business.

Protected Data or Information – Any TBI information/data that falls under the Secret/Confidential data classification as noted in the **TBI Data Classification Policy.**

Vendor – Third party supplier of products and services to TBI.

4) Document Ownership and Maintenance

The TBI GRC/Information Security team is the owner of this policy and is responsible for maintenance activities including reviews and revisions. It replaces all prior versions.

This document must be reviewed on an annual basis, (once per fiscal year), to ensure its continuing suitability, adequacy, and effectiveness. Modifications during the year will satisfy the annual review requirement.

5) Compliance

All TBI Users must comply with this policy in addition to all other Information Security policies and standards here: IT Compliance SharePoint site. Compliance to this policy will be verified through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner. Compliance verification methods will be in accordance with the applicable local laws. While utilizing TBI assets, user activity may be monitored for adherence to Corporate Policies.

Managers must regularly review the compliance of information systems and procedures within their area of responsibility with the appropriate TBI security policies and standards.

Exceptions must be documented and submitted for approval to grc@trueblue.com. Exceptions to the Information Security Policy will be reviewed and re-approved on a regular basis by the GRC/Information Security Team.

Any violation of this policy may result in disciplinary action, up to and including termination of employment.

For more information regarding the exception process, refer to section 'e' in the ***TBI Managed System of Internal Control Standard.***

6) Organization of Information Security

a) Information Security Governance

TBI has established a formal organization dedicated to the management, implementation and support of Information Security.

a) Executive Sponsorship

Through the provision of clear direction, support and necessary resources and the acceptance of Information Security responsibilities, TBI demonstrates evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the Information Security program and organization's security posture.

b) Internal Organization

i) All information security responsibilities must be defined and allocated.

ii) Conflicting duties and areas of responsibility must be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

iii) Appropriate contacts with relevant legal authorities must be maintained.

iv) Appropriate contacts with organizations or departments that maintain awareness of threat intelligence trends must be maintained.

v) Information security must be addressed in project management, regardless of the type of project.

c) Information Security Risk Management

TBI Information Security Program has defined operational processes consisting of policies, standards and procedures that facilitate the effective, consistent and on-going management of

risks related to Information Security and are in alignment with business, legal and regulatory requirements.

d) Information Security Risk Assessment

i) TBI has established a standardized process to assess the potential risks to the confidentiality, integrity and availability of information. Risk assessments may vary in scope; for example, a risk assessment may be performed for the whole company, parts of the company, a group of information systems, an individual information system, a group of system components, or specific services.

ii) Risk assessments will be performed at a minimum annually and as needed based on relevant changes and in accordance with a risk assessment process. The Information Security risk assessments are led by Information Technology's Governance, Risk and Compliance (GRC) group.

iii) New technology or changes to the usage of existing technologies must not be introduced without the review and approval of the GRC/Information Security Team.

iv) For more information, see the:

1. ***TBI Information Security Risk Assessment Standard***
2. ***TBI Information Security Management System (ISMS)***
3. ***TBI Change Management standard***

e) Vendor Risk Management

TBI periodically contracts with vendors to exchange data for business purposes. Such data exchanges introduce a level of risk that includes, but is not limited to, unauthorized data disclosures and damage or loss of data assets.

i) All vendors with whom TBI shares data or have access to TBI network and assets or TBI users have to access such vendors' environment must undergo a Security Risk Assessment performed by IT Governance, Risk and Compliance.

ii) Such vendors must adhere to all provisions outlined in:

(1) ***TBI Information Security Risk Assessment Standard***

7) Asset Management

b) Data Classification

vi) TBI must define and communicate data classifications for all data produced, stored, and transmitted. This must include defining an information classification scheme to communicate protection needs and priorities and ensuring that information assets receive the appropriate level of protection when stored, handled, accessed, or disposed of.

i) For more information, see the:

(1) TBI Data Classification Policy

a) Asset Inventory

i) Assets associated with information and information processing facilities must be identified and an inventory of these assets must be drawn up and maintained to define appropriate protection responsibilities.

ii) The asset inventory must identify assets relevant in the lifecycle of information, document their importance, and indicate ownership. The lifecycle of information must include creation, processing, storage, transmission, deletion and destruction. Documentation must be maintained in dedicated or existing inventories as appropriate. The asset inventory must be accurate, up to date, consistent and aligned with other inventories.

iii) For more information, see the:

(1) ***TBI Asset Inventory Standard***

b) Acceptable Use of Assets

i) TBI information, regardless of its stored medium, its location, or who is using it, will and always remain the sole property of TBI. Users must ensure through all means available that proprietary information is protected in accordance with the locally applicable data protection standards and regulations.

ii) Users are prohibited from using non-TBI-provisioned end-user devices to access the TBI networks and assets or conduct TBI business using them unless approved by Information Security.

vii) Only TBI-provisioned or TBI Information Security approved devices are permitted to connect to the TBI networks and assets.

iii) Users have a responsibility to promptly report the theft, loss or unauthorized disclosure of TBI-provisioned device or information to the Information Technology help desk at (800) 850-2558.

iv) Users may access, use or share TBI proprietary information only to the extent it is authorized and necessary to fulfill their assigned job duties.

viii) Users are responsible for exercising good judgment regarding the reasonableness of personal use. TBI has created guidelines concerning personal use of Internet/Intranet/Extranet systems. TBI reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy. TBI is not responsible for the loss of any personal data stored on TBI systems.

v) Users are responsible for the security of TBI assets provided to them or accessible by them, both physical and digital. TBI Restricted, Confidential and other sensitive business information on all media (paper, electronic storage media, etc.) must be secured at all times and not left on desks unattended, or at printers, or other common areas, especially when the office is vacated.

ix) Users are required to lock their screens or log off when devices are unattended in unprotected areas.

x) Users are expected to adhere to the same TBI security measures when working from home or at remote sites.

xi) User must not engage with any external third party to procure services for a TrueBlue provisioned asset without the involvement of technology asset management team.

xii) Users must comply with any other Acceptable Use Policies including GenAI AUP.

xiii) For more information, see the:

(1) ***TBI Acceptable Use of Assets Standard***

c) Data Privacy

i) To help TBI protect the privacy of our employees and members, production data must never be used in non-production environments (i.e. test/development) without prior approval from Information Security. Such approval must come for named period after which exception is no longer valid.

ii) Development, testing, and production environments must be separated to reduce the risks of unauthorized access or changes to the production environment.

iii) Restricted Data (including but not limited to Personally Identifiable Information) information that TBI obtains through the normal course of business may not be disclosed to anyone who does not have a business need to know.

iv) For more information, see the:

(1) ***TBI Company Data Privacy Policies***

8) Security Awareness, Education and Training

a) Awareness and Training

i) To ensure that employees are aware of Information Security threats and concerns, as well as their own responsibilities, TBI must have a security awareness and training program. Under this program:

(1) All employees will be required to review and acknowledge this policy upon hire, annually, and on significant updates. Additionally, as relevant to their job function, users of TBI network and assets have the responsibility to review other policies and standards as outlined in Policy Review Matrix section of this policy document.

(2) All employees will be required to complete quarterly security awareness training on various topics selected by the Information Security team.

(3) The Information Security team will run monthly phishing simulation campaigns to ensure consistent and on-going training.

(4) Users whose job function involves code design, development and deployment must complete any mandatory training on secure coding that they are enrolled in.

ii) For more information, see the:

(1) ***TBI Human Resources Policies***

9) Security Operations

a) End Point Malicious Software Detection and Protection

All Laptop, desktop, and servers must have end point protection software installed on all operating systems (Windows, Linux, Mac OSX, etc...). This software must provide anti-virus, anti-malware, and other protections from malicious software including:

i) Protection against tampering or uninstallation

ii) Only allowing changes to configurations by authorized individuals

iii) Receiving at least daily updates

iv) Providing host-based firewall controls that are actively running and restricted from changes by unauthorized individuals

v) Monitoring and alerting capabilities when any anomaly is detected by such software.

For more information, see the: ***TBI Malicious Software Management Standard***

b) Threat and Vulnerability Management

i) TBI must be proactive in protecting its resources against security exposures by implementing technical and organizational means to review the organization's IT infrastructure for vulnerabilities and identify threats.

ii) Workstations and servers owned and leased by TBI must have up-to-date operating system and application security patches installed to protect the asset from known vulnerabilities. This includes all laptops, desktops, servers, network devices and mobile devices owned/leased and managed by TBI.

iii) Procedures must be implemented to control the installation of software on operational systems.

iv) A Vulnerability Management program must be implemented and include the following:

(1) Identification and Classification

(a) Conduct regular vulnerability scans and assessments of all information systems (including infrastructure and applications) to identify vulnerabilities.

(b) Classify vulnerabilities based on their severity and potential impact using a standardized scoring system, such as the Common Vulnerability Scoring System (CVSS).

(2) Evaluation and Prioritization

(a) Evaluate identified vulnerabilities to determine the potential impact on TrueBlue's information systems.

(b) Prioritize vulnerabilities based on their severity, potential impact, and the criticality of the affected systems.

(3) Mitigation and Remediation

(a) Implement appropriate mitigation strategies to address identified vulnerabilities, including applying patches, configuring security settings, updating application code, and implementing workarounds.

(b) Develop and maintain a patch management process to ensure timely deployment of security patches.

(c) Document all remediation actions taken, including timelines and responsible parties.

(4) Monitoring and Reporting

(a) Continuously monitor information systems for new vulnerabilities and changes in the threat landscape.

(b) Report vulnerabilities and remediation efforts to relevant stakeholders, including IT management, security teams, and affected business units.

v) For more information, see the:

(1) ***TBI Patch Management Standard***

(2) ***TBI Vulnerability Management Standard***

c) Sharing of Information

i) Shared or communicated information is subject to several threats including, but not limited to interception, copying, modification, unauthorized routing, and destruction. Therefore, TBI must maintain the security of information shared both internally (within the company) and externally (outside of the company).

ii) Restricted or Confidential data must not be shared with an external entity without an Information Security assessment of the technology and risk to TBI computing environments.

iii) For more information, see the:

(1) ***TBI Data Asset Protection Standard***

(2) ***TBI Data Classification Policy***

d) Information Backup

i) To protect against loss of data due to a security incident, backup copies of information, software and system images must be taken and tested regularly in accordance with an agreed backup standard.

ii) For more information, see the:

(1) ***TBI Information Backup Standard***

e) Change Management

i) All changes to the TBI production environment must be strictly controlled using the change management process. A CR must be submitted, analyzed, and authorized prior to the implementation of a change. CRs must be assigned a change type based on their level of risk, history of like changes, and timeframe for which the change is needed. An emergency change process must be established for changes that cannot wait until the next change

meeting. TBI must review all CRs to ensure information security and compliance requirements are satisfied prior to authorization.

ii) For more information, see the:

(1) ***TBI Change Management Standard***

f) Logging and Monitoring

i) TBI must record events including logs of user activities, exceptions and faults

ii) Information security events must be logged and regularly reviewed

iii) For more information, see the:

(1) ***TBI Logging and Monitoring Standard***

10) Access Control

a) User Provisioning, Modification and De-Provisioning

i) TBI follows a formal user access management process for granting and revoking access to all information systems and services as appropriate to the classification of the information that such access would provide. All access which is not specifically allowed is implicitly denied.

ii) For more information, see the:

xiv) ***TBI Identity and Access Management Standard***

b) Unique Identification and Minimal Access

i) TBI provides access to authorized users on a “need to know” basis; access is sufficiently limited such that only the minimum level of access and duration is provided to meet a legitimate business need.

ii) Additionally, before granting permission to access a TBI asset or network, users must be uniquely identifiable for authentication and accountability purposes via a User ID, a secret password or passphrase and where applicable and required, a second factor in the form of an authentication code.

iii) Passwords or passphrases must never be shared or revealed to anyone with the exception of new hire onboarding

iv) For more information, see the:

(1) ***TBI Identity and Access Management Standard***

c) Management of Privileged Access Rights

i) The allocation of privileged access rights must be controlled through a formal authorization process.

ii) The privileged access rights associated with each system or process, e.g. operating system, database management system and each application and the users to whom access is granted, must be identified.

iii) Privileged access rights must be allocated to users on a need-to-use basis and on an event-by-event basis in line with the access control policy, i.e. based on the minimum requirement for their functional roles.

iv) An authorization process and a record of all privileges allocated must be maintained.

v) Privileged access rights must be assigned to a user ID different from those used for regular business activities.

vi) For more information, see the:

(1) ***TBI Elevated and Privileged Access Management Standard***

d) Requests for Access or Modification of Access

i) Only designated leaders can approve requests for, and modifications to, access.

ii) All requests for access or modification of access must be documented and retained.

iii) Requests from external entities (e.g., vendors, auditors, other third parties) must require approval.

e) Removal of User Access Rights

i) The access rights of all users to information and information processing facilities, systems, processes and services must be adjusted or removed upon change or termination.

f) Review of User Access Rights

i) Asset and/or system owners must review user access rights at regular intervals and after any changes, such as promotion, demotion or termination of employment.

ii) For more information, see the:

(1) ***TBI User Access Review Standard***

g) Authorization

i) Users must be granted access only with documented permission from designated authorities within TBI. TBI removes users upon notification of termination or transfer as soon as possible.

ii) For more information, see the:

(1) ***TBI Identity and Access Management Standard***

h) Identity and Access Management

i) Each user accessing TBI computing resources must have a unique User ID.

ii) The allocation of secret authentication information is controlled through a formal management process.

iii) Shared and Generic Identities must only be used in any environment if they are technically unavoidable and approved through the standard Information Security Exception process.

iv) For more information, see the:

(1) ***TBI Identity and Access Management Standard***

i) Authentication

i) Authentication mechanisms such as passwords are the primary means of protecting access to computer systems and data. All access into TBI network must require multi-factor authentication. Additionally, all TBI information systems must implement multi-factor authentication, where technically feasible. Exceptions must be requested and tracked through the exception management process.

ii) For more information, see the:

(1) ***TBI Identity and Access Management Standard***

(2) ***TBI Password Management Standard***

j) System and Information Access

i) To prevent unauthorized access to information, TBI must restrict access to systems based on the principle of least privilege and as approved by management access definitions.

ii) For more information, see the:

(1) ***TBI Identity and Access Management Standard***

k) Use of privileged utility programs

i) Utility programs capable of overriding system and application controls must not be used unless approved by IT Compliance.

l) Session and Account Inactivity

i) Inactive sessions must be locked or shut down after a defined period of inactivity no longer than 15 minutes.

ii) Accounts not accessed for 90 days must be disabled

iii) New user accounts not accessed for 30 consecutive days must be disabled

m) Wireless Access

i) TBI must provide secure wireless access to support the mobile computing capabilities of TBI-issued mobiles devices (e.g., laptops).

ii) Users must not deploy or install wireless access points into the TBI environment.

iii) Only authorized and approved devices will be allowed to connect to TBI Wireless networks.

iv) For more information, see the:

(1) ***TBI Wireless Access Management Standard***

n) Mobile Device and Remote Access

i) To manage the risks introduced by using mobile devices, TBI must implement security controls to ensure that business information is not compromised.

ii) Only approved and authorized devices with approved controls must be allowed to access TBI network and assets via a mobile device.

iii) For more information, see the:

(1) ***TBI Mobile Device Management Standard***

iv) To protect information accessed, processed or stored at teleworking sites, TBI must define the conditions and restrictions for remote access.

v) For more information, see the:

(1) ***TBI Remote Access Management Standard***

11) Information Systems Acquisition, Development and Maintenance

a) Secure Development and Support Processes

i) TBI must ensure that security is an integral part of both internally and externally developed information systems by defining security requirements and controls that must be addressed in the implementation or adoption of new systems and the enhancement or support of existing systems.

ii) For more information, see the:

(1) ***TBI Application Security Standard***

b) System Testing & Validation

i) TBI must ensure that adequate testing is performed during both the development of new information systems and changes to existing information systems. TBI must establish procedures and controls to protect any sensitive or classified information used for testing purposes.

ii) For more information see the:

(1) ***TBI Application Security Standard***

(2) ***TBI Data Classification Policy***

c) Encryption

i) TBI must protect the confidentiality, of information using cryptographic means as determined by risk assessments that consider the information classification of handled data.

ii) Users must never introduce their own encryption into the TBI environment.

iii) The use, protection, and lifetime of cryptographic keys must be developed and implemented through their whole lifecycle.

iv) Cryptographic controls must be used in compliance with all relevant agreements, legislation and regulations.

v) For more information, see the:

(1) ***TBI Enterprise Encryption Standard***

(2) ***TBI Cloud Storage Standard***

d) Third Party System Delivery

i) TBI must assess third party products or services prior to entering into contractual agreements as evidenced by completion of the Security Risk Assessment and formal approval of the vendor by Information Security.

ii) For systems being developed or provided by a third party for TBI, TBI must provide formal security requirements to the third party.

iii) TBI must supervise the development of the system and verify if the security requirements were met prior to accepting the system delivery and implementing the system in the production environment. Once a system is placed in production, TBI must regularly monitor, review and audit third party supplier service delivery.

iv) For more information, see the:

(1) ***TBI Information Security Risk Assessment Standard***

12) Information Security Incident Management

a) Incident Management & Response

i) All users must report suspected security incidents to the Information Technology Service Desk who will be responsible for notifying the appropriate Information Security personnel immediately upon identification.

ii) Only Information Security Managers or teams tasked with incident management must perform incident classification and determine subsequent incident management activities.

iii) Users must not attempt to independently verify or confirm when they receive a security warning or detect a vulnerability and report it immediately.

iv) TBI must have defined procedures for reporting incidents. Such procedures must be adequately communicated to all employees and parties of interest.

v) TBI must maintain an up-to-date Incident response plan to provide a guideline to teams responding to a security incident which provides roles and responsibilities of Incident Response Team members, and suggested steps that should be considered for each phase of Incident Response.

vi) For more information, see the:

(1) ***TBI Information Security Incident Management Standard***

(2) ***TBI Incident Response Plan***

b) Legal and Regulatory

i) TBI must comply with all relevant statutory, regulatory and contractual requirements related to information and security.

ii) TBI must explicitly define, document and maintain its compliance approach.

13) Compliance Monitoring

a) **Monitoring**

i) TBI must monitor employees, business processes and information systems to ensure compliance with Information Security policies and standards.

ii) TBI's approach to managing information security and its implementation (i.e. controls, policies, standards, processes and procedures) must be reviewed independently at planned intervals or when significant changes occur.

iii) For more information, see the:

(1) ***TBI Managed System of Internal Control Standard***

14) Physical and Environmental Security

a) **Physical Access**

i) To prevent unauthorized physical access, damage and interference to the organization's facilities that contain either sensitive or critical information, control security perimeters must be defined and used to protect those areas.

ii) For more information, see the:

(1) ***TBI Physical & Environmental Security Standard***

15) Policy Review Matrix

Policy Review and Attestation Matrix									
Policy #	**Policy Name**	**ITSD (US / India)**	**Network Team**	**Systems Team**	**Cloud**	**Unified Comm**	**Security**	**LoB IT**	**Contractors**
TBI-ISP-001	Infosec Policy	X	X	X	X	X	X	X	X
TBI-ISP-002	Data Classification	X					X	X	X
TBI-ISP-003	Gen AI	X	X	X	X	X	X	X	X
TBI-ISP-004	Backup Standard			X	X		X	X	X
TBI-ISP-005	Physical Security			X			X	X	X
TBI-ISP-006	Acceptable Use	X	X	X	X	X	X	X	X
TBI-ISP-007	App Dev Sec				X		X	X	X
TBI-ISP-008	Vuln Mgmt	X	X	X	X	X	X	X	X
TBI-ISP-009	Password Mgmt	X					X		

TBI-ISP-010	Encryption		X	X	X	X	X	X	X
TBI-ISP-011	Data Asset Protection	X	X	X	X	X	X	X	X
TBI-ISP-012	Sec Incident Mgmt	X	X	X	X	X	X	X	X
TBI-ISP-013	Electronic Physical Media Disposal	X					X		
TBI-ISP-014	Malicious Software	X	X	X	X	X	X	X	X
TBI-ISP-015	Patch Mgmt		X	X	X	X	X	X	
TBI-ISP-016	Identity and Access Mgmt		X	X	X		X		
TBI-ISP-017	Mobile Device Mgmt	X	X	X	X	X	X	X	
TBI-ISP-018	Remote Access	X	X	X	X	X	X	X	X
TBI-ISP-019	Wireless Access Mgmt	X	X				X		
TBI-ISP-020	Cloud Storage			x	x		X	x	
TBI-ISP-021	Info Sec Risk Assessment		x	x	x		x	x	
TBI-ISP-022	Managed System of Internal Controls						X		
TBI-ISP-023	UAR	x	x	x	x	x	x	x	
TBI-ISP-024	Change Management	x	x	x	x	x	x	x	x

16) Associated TBI Security Policies and Standards

Policy	Standard	Owner
Information Security Policy		GRC/InfoSec
	Acceptable Use of Assets Standard	GRC/InfoSec
	Application Development Security Standard	IT DevOps, GRC/InfoSec
	Asset Inventory Standard	IT Infrastructure
	Cloud Storage Standard	GRC/InfoSec
	Data Asset Protection Standard	GRC/InfoSec
	Electronic Media Disposal Standard	GRC/InfoSec
	Elevated and Privileged Access Management Standard	GRC/InfoSec
	Enterprise Encryption Standard	GRC/InfoSec

Policy	Standard	Owner
	Identity and Access Management Standard	IT Infrastructure, GRC/InfoSec
	Information Backup Standard	IT Infrastructure
	Information Security Incident Management Standard	GRC/InfoSec
	Information Security Risk Assessment Standard	GRC/InfoSec
	IT Change Management Standard	IT Service Management
	Logging and Monitoring Standard	IT Infrastructure, GRC/InfoSec
	Malicious Software Management Standard	GRC/InfoSec
	Mobile Device Management Standard	IT Infrastructure, GRC/InfoSec
	Password Management Standard	GRC/InfoSec
	Patch Management Standard	GRC/InfoSec
	Physical & Environmental Security Standard	IT Infrastructure, Facilities
	Remote Access Management Standard	IT Infrastructure, GRC/InfoSec
	User Access Review Standard	GRC/InfoSec
	Vulnerability Management Standard	GRC/InfoSec
	Wireless Access Management Standard	IT Infrastructure, GRC/InfoSec
Company Data Privacy Policies		Legal
	Data Classification Policy	Legal
Records Retention Policy		Legal
Human Resources Policies		HR

17) RACI

Role	Activity							
	Information Security	HR	Information Technology	All Departments	Internal Audit	Legal	Executive Management	Contractors/ Vendors
Development	**A**	**---**	**C**	**---**	**C**	**---**	**I**	**---**
Enforcement	**R/A**	**C**	**C**	**---**	**C**	**C**	**I**	**---**
Monitor/Review	**A**	**---**	**R/A**	**R**	**R**	**C**	**C**	**R**
Conformance	**---**	**I/C**	**R/A**	**R**	**---**	**C**	**C**	**R**
Responsible | **A**ccountable | **C**onsulted | **I**nformed								

18) Revision history

Refer to Certificate of Review (last page).

Version	Description	Revision date	Name	Title
1.8	Annual review and updates	April-2024	Jose Herrera Dae Kim Vatsala Dubey Jennifer Johnson Chris Schweigert	Sr. Cybersecurity Engineer Cybersecurity Architect VP, Information Security (CISO) Director, Technology GRC Sr. Director, Security Operations
1.7	Annual review and updates	10-August-23	Jose Herrera Dae Kim Vatsala Dubey Jennifer Johnson Chris Schweigert	Sr. Cybersecurity Engineer Cybersecurity Architect VP, Information Security (CISO) Director, Technology GRC Sr. Director, Security Operations
1.6	Reviewed; no changes to content	11-July-2022	Mat Saunders Chris Schweigert Jennifer Johnson	SVP, Corporate Technology Senior Director, Security Operations Director, Technology GRC
1.6	Compliance section updated	21-May-2021	Jennifer Johnson	Director, Technology GRC
1.5	Reviewed; no changes to content	7-May-2020	Jennifer Johnson	Director, Technology GRC
1.5		30-May-2019	Byron Raynz	Sr. GRC Analyst
1.45	Final edits	27-Nov-2018	Karen Holmes Scott Bruce Duncan	VP, IT Compliance & CISO Lead Information Security Analyst
1.44	Comments added to new policy draft	18-Oct-2018	Ray Beaudoin	IT Compliance Manager
1.43	Comments added to new policy draft	26-Sep-2018	Byron Raynz Karen Holmes	Senior Manager, IT Governance and Compliance Sr Director, Information Security & GRC
1.42	Adoption of ISO/IEC 27001/2:2013 framework (policies & standards)	24-Sep-2018	Scott Bruce Duncan	Lead Information Security Analyst
1.41	12.f – Password Rules; (updated)	08-Sep-2017	Scott Bruce Duncan	Lead Information Security Analyst

Version	Description	Revision date	Name	Title
1.8	Annual review and updates	April-2024	Jose Herrera Dae Kim Vatsala Dubey Jennifer Johnson Chris Schweigert	Sr. Cybersecurity Engineer Cybersecurity Architect VP, Information Security (CISO) Director, Technology GRC Sr. Director, Security Operations
1.3	**Updated:** 9.a - Mobile Devices; 12.d - Review of User Access Rights; 12.f – Password Rules; 12.h - Operating System and Network Access Control; 12.i - Application Access Control; 12.l - 3rd Party Access Control; 14.a - Physical Security Controls; 15.a - Change Management; 15.j - Vulnerability Management; 16.d - Network Connection Control; 18.a - Information Security in Supplier Relationships (moved to 12.l – 3rd Party Access Control) **Added:** 12.b - System Administrators; 12.c – Segregation of Duties; 12.k - Program Source Library Access Control; 12.j - Direct Data Access Control; 15.k - Routine Systems and Batch Jobs; 19 - Exceptions management;	20-Aug-2016	Scott Bruce Duncan	Lead Information Security Analyst
1.2	Updates to draft	11-Dec-2015	Brett Morgan	Security Analyst
1.1	Revision of initial draft	09-Dec-2015	Hemal Sura	CISO
1.0	Initial draft	23-Sep-2015	Hemal Sura	CISO

19) -Approvals

Refer to Certificate of Review (last page).

20) Sources

This document has been implemented as mandated by and/or in support of the following policies and/or standards:

xv) **ISO/IEC 27001: 2022**, Information technology — Security techniques — Information security management systems — Requirements

xvi) **ISO/IEC 27002:2022**, Information technology — Security Techniques — Code of practice for information security controls

b) **ITIL V3 Supporting Information**

i) RACI Model: Responsible, Accountable, Consulted, Informed

Certificate of Review

Information Security Policy - v.1.9

March 25th 2025 9:12:39 am

Name	Job title	Stakeholder type	Action	Timestamp
Chris Schweigert		Policy Owner	Submitted	Wednesday, February 26, 2025 8:14 AM PST
Vatsala Dubey		Policy Owner	Submitted	Friday, March 7, 2025 4:19 AM PST
Jennifer Johnson		Policy Owner	Submitted	Friday, March 7, 2025 11:53 AM PST
Vatsala Dubey		Policy Approver	Approved	Friday, March 7, 2025 1:37 PM PST
Jennifer Johnson		Policy Admin	Published	Tuesday, March 25, 2025 9:12 AM PDT