Capri Global Capital Limited

Information & Cyber Security Policy

Policy Document – Ver 1.0

This document is reviewed and approved by "Members of Company Board" during board members meeting held on November 4, 2022

Purpose

The purpose of "Information & Cyber Security" policy is to define framework and provide guidance for IT team to secure corporate IT systems and application in accordance to regulatory requirements to protect and maintain integrity of corporate data.

Scope

Information & Cyber Security (IS) policy is group-wide master policy and applicable to all IT / non-IT functions assumed under businesses of all Capri Global legal entities. This policy is applicable and enforced to all persons including but not limited to employees, executives, board of directors, contractors, consultants or any third-party resources working for Capri Global on-site or has access remotely.

Revision Control

Version	Description	Action	Date	By
1.0	Rewrite Draft	Prepared	10-Oct-2022	Chinmay Parab

Reviewed By

Version	Name	Designation	Date	Sign
1.0	Bhavin Patel	VP – IT Infrastructure	12-Oct-2022	Bhavin Patel Digitally signed by Bhavin Patel Date: 2022.12.26 12:20:30 +05'30'
1.0	Nelson Mathews	SVP – IT Applications		Nelson Mathews Digitally signed by Nelson Mathews DN: cn=Nelson Mathews, o=Capri Global Capital Ltd, ou=Information Technology, email=nelson.mathews@capriglobal.in, c=IN Date: 2022.12.30 13:51:24 +05'30'

Approved By

Version	Name	Designation	Date	Sign
1.0	Rahul Agarwal	Chief Technology Officer		Rahul Agarwal Digitally signed by Rahul Agarwal DN: cn=Rahul Agarwal, o=Capri Global Capitals Ltd, ou=Technology, email=rahulcc@capriglobal.in, c=IN Date: 2023.01.02 12:16:59 +05'30'

Next Review Schedule

Version	Author	Review Interval	Last Review	Next Review
1.0	Chinmay Parab Information Security Officer	1 Year	Oct-2022	Oct-2023

Contents

1 Introduction

Information Security is not only about securing information from unauthorized access. Information Security is basically the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. Information can be physical or electronic one. Information can be anything, including but not limited to business procedures, system configurations, customer details, key data storage locations etc. Thus, Information Security spans across all verticals and covers every aspect of IT Systems etc.

"Information Security" policy is a statement of management intent which provides framework and guidelines by using rules and procedures for Capri Global IT systems and data security. This policy is a guide for Capri Global IT team on designing, implementing & management IT systems and services to allow the access, process and storage of information critical to Capri Global business operation in accordance with appropriate standards, laws and regulations.

1.1 Policy Statement

Capri Global must implement technical, procedural, administrative and operational controls at all levels to protect the Confidentiality, Integrity, and Availability of information stored and processed on its systems and ensure that information is available to authorized persons as and when required.

1.2 Responsibility of Information Security

While Capri Global IT Security function leads the Information Security operations, the responsibility of maintaining data security and integrity lays with every individual who has direct or remote access to or involved in planning, designing, implementing and operating Capri Global IT systems and its data storage locations.

This includes on-roll employees as well as all external contractors, and other third parties, who are associated with Capri Global IT function.

1.3 Compliance with IS policy

Business heads and functional owners of the application and technology should support regular reviews, at least once in a year for compliance of the systems and processes with the Information Security policy. Additional sections or guidelines may be issued as needs arise and will be incorporated into Information Security policy document during the renewal periods.

All employees, contractors, dealers, vendors, third parties and any other staff, who is a part of service agreement with the Capri Global, shall be responsible to ensure that Customer data, personal data and organization's data is not exposed to data leakage, theft, unauthorized access or spread of Viruses and malware into organization's network.

Refusal to comply with or violation of information security policy could result in a penalty/punitive action, depending upon the context and severity of breach that may include, but not limited to Warning/Caution, Suspension, Termination or Legal Proceedings.

2 Information Security Policy

As Information security touches every function of business and IT department, information security policy has various sections to address specific requirements of individual functions security areas and together, all these sections form a consolidated and comprehensive Information Security Policy.

2.1 Document Control

Documents are major source of information in any enterprise and Capri Global is no exception to it. Many documents are being formulated or have been created to record very unique and sensitive information about companies' business model and strategy, underline IT systems and security configurations. If not protected properly, loos documents could lead to major risk to information security.

- Roles and responsibility of formulating/managing/authorising information sensitive documents must be clearly defined and approved by TOP management of Capri Global.
- A document must contain relevant information to quantify its existence and relevance into Capri Global. Document must have details like Title, Classification, Owner, Author, Approver, Reviewer, Date of Publishing, Version details, Approval Status, Circulation List and References.
- All these fields are mandatory and must be filled with relevant and correct information.
- Documents must be classified / stored and circulated according to approved process note.
- Unclassified and Untagged documents must not be published or circulated. Such documents shall not be considered as authentic under Document Control process.
- Document author can not be reviewer or approver; Capri Global must identify individuals or committee to review and approve documents. All approvals must be recorded on document in digital or physical signed format.
- Approved document contents cannot be changed unilaterally; all amendments/changes must be tracked and recorded under document revision control and should undergo reapproval process before publishing amendments as final document.
- Every document must have defined review period, not exceeding one year. Reviewed document must be re-signed by approving authorities to affirm reviewed copies.
- All signed documents must be published and made accessible to targeted audiences only.
- Document which became irrelevant or unapplicable shall be taken out from document repository.
- Approved copies of documents must be made available to internal / external auditors during audit period or as situation demands.
- Record of all documents, approved as well as discarded must be maintained for document governance and tracking purpose.
- Physical copies of documents must not be left unattended; all such documents should be shredded immediately after use.
- Unauthorised access, download, share of secured documents from repository is strictly prohibited. Identified individuals violating this policy will face strict action.

2.2 Password Security

Passwords are very sensitive and critical components under Information Security. Weak or unregulated passwords could lead to severe security risk like system compromise, intrusion, or data theft. Password of any user account including but not limited to Employee id, application id, network devices id, database user, used in Capri Global network must meet Password Policy of Information Security.

2.2.1 Password policy

- Passwords should be consisted of minimum eight characters.
- Passwords must be complex and should include alphanumeric and mixed case characters i.e., at least one integer (0-9) and one special character (! @ # $ % ^ & * ( ) _ + | ~ - = \ ` { } [ ] : " ; ' < > ? , . /) as well as both upper- and lower-case letters of the alphabet.
- The password should not contain the user's name or user-ID or other easily guessable combinations.
- A password must not be created or have common, guessable strings such as @123, @2015, birthdate or name of self, family, pet.
- System must maintain password history and shall not the same password to be repeated within a cycle of 13 password changes.
- Password must have max age of 90 days, before forcing users to change password.
- System must notify users about password expiry or IT team shall setup communication channel to made users aware about password expiry.
- Password for any user account must not be changed unless formal request received from authentic user. IT team must maintain record of all requests for change / reset password.
- Initial password shared by IT administrator or helpdesk personals must be change as soon as possible by user.
- System must have capability to allow users to change their account password on the login interface (after authentication) and the session must be re-authenticated with the new password.
- Both user-ID and password must be authenticated before allowing access to Capri Global systems and / or applications.
- Authentication failure message to user shall be indicative such as "Incorrect login" or “Incorrect user-id or password” and not exact such as "Incorrect password".
- Ideal sessions on desktops and servers should be lock-out at 15 minutes and 5 minutes of inactivity respectively.
- While entering a password it should be masked/hidden and not be visible on the screen.
- User account ID should be locked after the 3 unsuccessful login attempts and should be unlocked by the system administrator manually on approvals.
- User passwords can be shared via a text message on a mobile number to user or to the immediate Reporting Manager on Reporting Manager’s official email account in one-on-one communication.
- Sharing and disclosing passwords in open email or other group channels is violation of password policy and strictly prohibited and such exposed account passwords must be changed immediately.
- System account passwords must not be hardcoded in software/application/utility in cleartext or in human readable format.
- User must maintain complete secrecy about their account passwords and must not share, post, write, or otherwise divulged it in any manner to anyone.
- One user account & password must not be used by multiple users, for any reason. Shared use for credentials is not permitted and is violation of this policy.
- Any user suspecting that their password may have been compromised should immediately change the password and report it to the Information Security officer.
- Audit trails should be maintained by the administrator for all events related to password management. The audit trail must be periodically reviewed for anomalies and resolved promptly.
-

2.3 Malware Protection

Malware protection is essential and mandatory for all systems including endpoints/laptops/desktops. Capri global IT systems and its data must be protected from any kind of risk involving threats like but not limited to virus, trojans, spyware, ransomware etc

2.3.1 Malware detection & prevention

- All internal/ external clients and servers connected physically or remotely to Organization's network shall have anti-malware software installed, configured, activated and updated with the latest version of the malicious code definitions before or immediately upon connecting to the network.
- Anti-malware software on all endpoints must be centrally managed and configured according to this policy.
- Anti-malware software should be capable of detecting, containing, removing, and protecting Capri Global data against any forms of malicious software, including spy ware, ransomwares etc.
- New definition signature updates should be applied to all endpoints as soon as, released by vendor. There should be proper monitoring of the updating of the signatures on servers and clients.
- Antivirus should be configured to perform a full scan on all endpoints at least once a week; it should be properly scheduled, preferably during the lean period of office hours.
- Antivirus must be configured to perform real time scan of all the files as and when they are opened, copied or moved.
- All the emails and its attachments must be scanned as it enters the Capri Global network and before it leaves the server.
- If malicious code is found, the email should be quarantined for investigation by IT team without any notification to the recipients.
- Anti-malicious code solutions shall be installed on the internet gateways for scanning the internet requests for malicious code, software, applets, ActiveX etc downloaded from Internet.
- Users should report to system administrator / helpdesk for any abnormal behaviour of the system or in the event virus is not getting cleaned by the anti-virus agent.
- Disabling / deactivating malware protection is strictly prohibited; IT team must configure security control to prevent disabling or uninstall of malware protection software without proper authorization.
- Capri Global IT team must practice techniques and tools to detect/report/protect unprotected endpoints automatically.
- Any detection of malicious activity on endpoints must be recorded under cyber security incident and tracked according to its impact or affected endpoints.
- Capri Global IT shall configure IT systems and networks to prevent lateral movement malware infection; any infected system must be isolated from Capri Global network immediately and reconnected only after completely cleaned or formatted.
- Statistical report on malware protection must be published and shared with IT leadership team at periodic interval.

2.4 Secure Configuration Policy

IT systems are backbone of modern corporate world. While there are immense benefits of running business through digital platform but it also has its own security risks which could lead to severe threats like but not limited to data theft, identity theft, malware attack which could result into loss of reputation and revenue for any organization.

Secure configuration policy deals with risk areas of IT systems security to reduce attack surface and avoid weak configuration.

2.4.1 Objective

The goal of secure configuration policy is to ensure installed IT systems including servers, databases, network devices meet minimum security parameters to avoid security lapse/weakness in Capri Global IT services.

2.4.2 Policy Details

- Installation and management of all IT equipment/applications in Capri Global must comply to "IT System & Operations" policy.
- Only required and necessary services to be allowed to run on production servers. All servers must be hardened according to approved server hardening process to reduce threat surface attack.
- Production servers must be firewalled and separated from non-production server workload. Only necessary ports should be allowed from external network to subnets running production servers and databases.
- Any alteration/change in network access rules for production workload must be reviewed and authorised by Information Security Officer or IT Infra head followed by change management process.
- Internet access on servers must be restricted. By default, no server will be allowed to connect internet directly. If required, only specific URL/IP must be allowed to connect after thorough review and approval Information Security Officer / IT Infra Head.
- Removable storage access on all servers must be disabled. If situation demands, such access can be activated for temporary period only after approval from IT Head / CTO.
- Unsecure web servers/APIs should not be allowed to run on Capri Global network; there must be SSL/TLS level protection to secure these services.
- Weak SSL/TLS protocols & chippers must not be actively disabled / removed to enforce strong encryption for in-transit traffic.
- Data on-rest must be encrypted to prevent unauthorised access. This is applicable to in-use production data as well as backup copies.
- Any threat detection / suspicious activity on corporate devices must be tagged under cyber security incident and must be investigate thoroughly to inspect and envisage impact on Capri Global IT.
- Default ID/password on servers / network devices must be renamed/disabled. Only delegated admin ID must be used to manage/operate IT tasks.
- Privileged IDs/access must be strictly governed and tracked for access to production systems.
- Corporate network must be secure to deny access to unauthorised/unknown devices.
- Broadcasting unsecure wifi on Capri Global network is strictly prohibited. IT team must set policies/processes to prevent configuration of unsecure wifi/wireless hotspots.
- Any access to IT systems management console must be controlled; it must be limited to and allowed from identified secure workstations only.
- Capri IT team and Information security officer must review the configuration of IT systems at periodic interval to identify and fix security gaps.
- Application codes / integrations must not store passwords in human readable format; rather it should be encrypted.
- Capri global IT team must prevent open file shares on company network. Such shares are first target of attackers to spread malicious codes. Such shares must be restricted or stopped to prevent lateral movement of treat infection.

- All security agents / services must be tamperproof; services like antivirus, encryption, web access agent must not be allowed to be disabled/deactivated by users/local administrators.

2.5 Log Management

Almost all IT systems generate various types of logs during operational activities. These logs are very essentials as it contains useful information about events happened during operation of IT services and are very crucial for forensic analysis to trace root cause.

2.5.1 Objective

The goal of this policy is to define framework for effective log management of Capri Global IT systems and provide guideline for Capri Global IT team to capture, store and analyse logs generated by servers, applications, databases, network devices etc.

Log management can be of great benefit in a variety of scenarios, with proper management, to enhance security, system performance, resource management, and regulatory compliance. Capri Global will perform a periodic risk assessment to determine what information may be captured from the following:

- Access – who is using services
- Change Monitoring – how and when services were modified
- Malfunction – when services fail
- Resource Utilization – how much capacity is used by services
- Security Events – what activity occurred during an incident, and when
- User Activity – what people are doing with services

2.5.2 Policy details

2.5.3 Log Configuration

- All production systems should be configured to capture audit logs to track critical events like stop/start any service, system shutdown event, failed attempts and successful login events, access audit logs, application events etc along with timestamp of event and source system/IP.
- All logs source must be secured from unauthorised access/deletion. Any such action must be logged to indicate changes executed in log files.
- Anti-malware logs must be enabled on every system to capture events of protection enable/disabled, full scan performed, definition/software update, detected malwares, file and system disinfection attempts, files quarantined etc
- Intrusion detection/prevention system events must be logged to collect information about suspicious behaviour of processes, identified attacks, actions performed by intrusion prevention system to stop the malicious activities or source.
- Events of all the access through web firewall/gateways should be logged. These logs should include but not limited to all the URLs accessed through web gateway, outbound requests and incoming responses, source of traffic, general classification of web destination, user details and timestamp.
- All events of authentication servers including active directory servers and single sign-on servers should be logged. These logs must include information about but not limited to each authentication attempt, origin of authentication attempt, target service/port, username, success or failure, timestamp.

- Events of all the access through network firewall should be logged. These logs must include complete details of outgoing requests, source/destination IP address, source/destination port/protocol, connection timestamp, policy/rule applied and action taken.
- Application servers must log events about to the user authentications, requested URLs, server responses, records accessed by user, actioned performed and timestamp.
- Database servers must log events related to DB user authentication, connection source, client version/type, action performed/queries executed by users, session period etc.
- Wireless equipment must log events about connecting devices type, MAC ID, timestamp of connections, action performed on connection etc.
- Administrative actions/events also to be logged in systems log such as administrator login/logoff, action performed and timestamp.

2.5.4 Log management & analysis

- All production system logs mentioned under log configuration or other which are necessary, must be captured and stored in centralised log (syslog) management system.
- Syslog solution must collect, monitor and analyse logs in compliance to regulatory mandates.
- Data collected in syslog must be tamperproof; modification/deletion of logs should not be allowed.
- All collected log data must be retained for at least 90 days in log management system and older data can be moved into archive before purging after 365 days.
- Care should be taken not to retain log records that are not needed. The cost of long- term retention can be significant and could expose Capri Global to high costs of retrieving and reviewing the otherwise unneeded records in the event of litigation.
- At any given point of time, IT team must be able to extract and share evidences on IT log management to internal of external auditor.
- Information security officer/function shall monitor the log database actively to unearth possible threat attacks/data leak on Capri Global IT system.
- IT Operations team along with Information security officer/function is responsible for effective management of IT logs and log management system.
- Statistical report on IT system logs must be shared with IT leadership team at regular interval.

2.6 Vulnerability assessment

2.6.1 Overview

Vulnerability assessment, at Capri Global are necessary to manage the increasing number of threats, risks, and responsibilities. Vulnerabilities are mainly related to security loopholes and bugs in softwares/operating systems/applications, if not fixed on time, these vulnerabilities could cause big risk to IT systems and may result in loss of reputation and revenue.

2.6.2 Objective

The goal of this policy is to establish a standard framework for periodic vulnerability assessments of Capri Global IT systems. This policy reflects Capri Global's commitment to identify and implement security controls, which will keep risks to information system resources at reasonable and appropriate levels.

2.6.3 Policy details

- This policy covers IT devices like web/application servers, database servers, network devices like firewall/wireless devices owned or operated by Capri Global.

- Vulnerability assessment is a mandatory process and shall be performed for all in-scope applications/servers/IT devices.
- New deployments/major code changes must undergo vulnerability assessment to confirm system is secure enough to run production workload.
- Vulnerability assessment of production systems must be performed from internally as well as externally to provide maximum coverage of risk exposure as VA tool able to scan all the services and ports from internal network.
- Vulnerability assessment must be run against all services/applications/ports open/available on IT devices.
- To ensure vulnerabilities are adequately addressed, the operating system or environment for all information system resources must undergo an authenticated vulnerability assessment.
- IT must define fixed matrix of vulnerability assessments according to application criticality; this schedule must be clearly defined in approved vulnerability assessment process note.
- VA results must be revalidated to ensure applied mitigation have fixed the open risks. A system generated report must be published to confirm system health.
- Vulnerability reassessment period of business-critical workload shouldn't be longer than a quarter.
- Vulnerabilities must be categorised and high severity observations should be fixed on priority.
- While vulnerabilities mitigation is important, impact of the changes must be validated first in non-production environment before moving the changes into production.
- Mitigation related to application components major version upgrade and database service packs must be carefully executed as it may destabilize whole application.
- All data collected and/or used as part of the vulnerability assessment process and related procedures to be formally documented and securely maintained.
- Running applications/workload with known vulnerabilities is big risk and violation of "Information Security" policy.
- Information security officer/function assisted by IT operations team are responsible for maintaining vulnerability free system in Capri Global network.
- Any deviation under this policy must be documented and approved by IT Head / CTO with defined time to revisit the risk acceptance.
- Statistical report on IT systems VA health status must be shared with IT leadership team at regular interval.

2.7 Patch Management

2.7.1 Overview

Patch management is key process of IT security operations. Security vulnerabilities are inherent in computing systems and applications. These flaws allow the development and propagation of malicious software, which can disrupt normal business operations, in addition to placing Capri Global at risk. In order to effectively mitigate this risk, software "patches" are made available to remove a given security vulnerability.

2.7.2 Objective

This policy works as guideline for Capri Global IT team to identify, list and patch known vulnerabilities on all IT systems including endpoints, servers, applications, databases and network devices.

2.7.3 Policy details

- Patch management can not be selective; all components including operating systems, softwares, 3rd party applications must be checked for missing security updates.
- Tool use for patch management must be equipped with continuous scanning, detecting, reporting and mitigating know security/non-security updates on various endpoints & applications including Windows as well as Linux & MAC.
- Patches must be ranked and priorities for deployment according to severity, scope and relevance.
- Patch management must follow staged approach, all patches must be deployed in non-production systems before deploying it on production environment.
- Change management process must be followed to record changes done on production systems.
- Approved patch management process must clearly define acceptable level of patch levels to tag systems as healthy, vulnerable or highly vulnerable.
- All patches must be deployed at earliest possible time; IT team must have defined schedule for patch deployment cycle under approved process note.
- If any zero-day patch for critical vulnerability released, IT team must take steps to apply it on priority basis.
- All newly configured endpoints/servers/network device must be running latest version of security/non-security patches before commissioning into Capri Global network.
- Failure to properly update new system is a violation of this policy. Disabling, circumventing, or tampering with patch management protections and/or software constitutes a violation of policy.
- Unsupported / outdated softwares must not be allowed to run on system; IT team must take adequate measurements to handle such legacy softwares.
- Post patch deployment, IT systems can be restarted/force to restart, provided prior notification and communication send to respective device owner or stakeholders.
- Information security officer/function assisted by IT operations team is responsible maintaining adequate security level of Capri Global IT systems.
- Any deviation under patch management process must be clearly documented and approved by IT Head/CTO with defined period of risk acceptance.
- System generated statistical report on IT systems patch health status must be shared with IT leadership team at regular interval not exceeding 1 month.

2.8 Mobile device management

2.8.1 Overview

Mobile devices have become major component of modern enterprise business functions as multiple apps are being designed/developed to work on mobile devices for ease of operation and improvise business functions. Organizations also promotes use of personal mobile devices for business operation purpose to take benefits of mobile technology but this has open new angle of security risks and if not handled properly, could lead to severe risks like data leak, theft and revenue loss.

2.8.2 Objective

This policy has aim of standardising framework to allow permissible use of mobile devices for operating, storing and accessing Capri Global company data, applications, emails on mobile devices.

2.8.3 Policy details

- Only use of personal mobile devices is permitted under BYOD process to access, operate and store company data.
- Personal devices like laptops, notebooks are not permitted and shall not be used to connect Capri Global network.
- All mobile devices including personal and company provided, must enrol to Capri Global mobile device management before gaining access to Company IT services.
- MDM solution must be centralised platform to control, govern and discard mobile devices from Capri Global. This solution will capture relevant information like IMEI number, device model, OS, storage, applications, location, battery information to effectively manage enrolled devices.
- Authorised user is permitted to enrol only one mobile device in company MDM solution; if situation demands, additional device enrolment can be allowed followed by approval from IT Infra Head.
- MDM solution must be configured to authenticate user first, before allowing them to enrol their mobile devices.
- For BYOD devices, mobile device must support containerization to isolate company work files from personal profile. Company data / files must not be visible / sharable with other apps on personal profile.
- Company owned devices must be enrolled as device owner and fully managed by MDM policies, allowing user only functions/applications necessary to complete tasks to support job role.
- MDM enrolled devices must be restricted from transferring/copying company data/files using channels like WIFI, Bluetooth, share apps, OTG storage etc.
- Screenshot on work profile is prohibited and any such attempt is violation of this policy.
- Users enrolling to Capri Global MDM service must accept MDM policy and agree keep their usage in accordance to 'Acceptable Usage' policy defined under 'Corporate IT Policy'.
- MDM enrolled corporate devices / work profiles must not be allowed to download, deploy application / softwares from unknown sources. Only whitelisted application approved by Capri Global IT team should be permitted to run on MDM enrolled devices.
- Non-compliant, rooted, jail broken devices are not be allowed in Capri Global. If detected, Capri Global IT team reserves rights to take appropriate action to delete corporate data on such devices without prior notice.
- Users are responsible and accountable for safekeeping company data on personal devices. Any incident led to data risk like device lost, theft/stolen must be immediately notified to IT Team.
- Capri Global IT team has responsibility of disabling access to and delete work profile for users leaving organization.
- Capri Global IT team reserves right to completely wipe enrolled devices to protect and maintain integrity of corporate data.

2.9 Data security & recovery

2.9.1 Overview

Data is at the heart of any organization and information systems are main source of company's data store. IT system produce, process and store business critical and customer related information which must be protected and maintained in a manner to avoid loss of data which could risk organizations business function and lead to revenue loss.

2.9.2 Objective

The goal of this policy is to identify and report possible risk areas for data security in term of data storage and recovery prospective. This policy defines framework to manage 'data at rest', 'data in transit', 'data sharing within the organization', 'data sharing outside the organization', 'data backup & restore' etc.

2.9.3 Policy details

- All IT device's storage location used for storing company data must be encrypted using strong disk level encryption.
- By default, access to removable storage devices must be prohibited on all endpoints. Exception can be allowed post necessary approvals from authorities.
- Access & ownership of removable storage devices must be tracked and reviewed at periodic interval.
- Data in-transit between endpoints and applications must be secure by applying session encryption technology like transport level security (TLS) 1.2 and above.
- All weak ciphers and protocols must be disabled; application/endpoints should be configured to work on latest version of TLS security.
- Key management procedures should ensure that only authorized users can access and decrypt all encrypted data using controls that meet operational needs and comply with data retention requirements.
- Key management should include but not limited to key generation, distribution, storage, archiving, destruction, revocation and recovery when lost or corrupted.
- Data in-transit between branch locations and datacentre must be secure by applying tunnel encryption technology like site-to-site IP-Sec tunnel.
- Use of unsecure file sharing tools like Bluetooth connectivity, WiFi hotspot, 3rd party apps like Shareit is prohibited and such services must be disabled/removed during commissioning of asset.
- User performing data sharing with internal company users must be cautious and must not be share data with irrelevant user / department. Marking unnecessary mails with large number of recipients is not appropriate and shall not be done.
- Internal share folders must not allow access to anyone/everyone. Only authorised users must be allowed to connect basis defined process.
- Share folder access containing highly critical and sensitive data must be logged under access audit mgmt.
- Data sharing with user outside organization is not permitted and should be blocked. If necessary, IT team can temporarily allow this access followed by specific approval from authorities.
- Deliberate attempt to share data is violation of Capri Global Corporate IT Policy, IS Policy and would attract to strict action against involved users.
- Company data must be always backed up inline to backup policy at regular interval and stored in separate encrypted storage or password protected repositories. Recovery of data from backup file must be authorised through secret passphrase.
- Access to backup data must be restricted and only authorised persons from IT team should be allowed to view and recover data from backup repositories.
- Capri Global IT team must take periodic review of backed up data and verify its recoverability time to time basis.
- Any deviation on data security policy must be documented and approved by IT Head/CTO with defined date to revalidate.

2.10 Access Security

2.10.1 Overview

"Access management" is critical process for Capri Global information security. Effective control on access management allows IT team to reduce risk by preventing unauthorised access to business-critical data, IT equipment and systems.

It is essential to develop and implement system and procedures in order to safeguard information and computing resources from threats like unauthorized access, modification, disclosure or destruction thereby, ensuring that information remains accurate, confidential and is available when required.

2.10.2 Objective

The purpose of the "Access Security Policy" is to establish the requirements necessary to ensure that access to and use of Capri Global IT resources is managed in accordance with business requirements, information security requirements, and other Company policies and procedures.

2.10.3 Policy details

- Capri Global encourages role-based access control mechanisms, with unique user-ids attached to roles. In all cases, the employee/ contract staff user identification number must be associated with every access mechanism.
- Access to Capri Global IT systems should be allowed according to approved process only. No service, system should allow default or unauthenticated access to anyone.
- Access delegation must follow the rule on least privilege, only the level of access required to perform authorized tasks may be approved.
- Ownership of IT systems and service must be defined and documented. Access to critical and sensitive IT systems is based on 'need to know'.
- All accounts created must have an associated, and documented, request and approval.
- Segregation of duties must exist between access request, access authorization, and access administration.
- Information Resource owners are responsible for the approval of all access requests. Respective stakeholders must take conscious decisions while reviewing and approving any access request.
- User accounts and access rights for all Capri Global IT Resources must be reviewed and reconciled at least annually, and actions must be documented.
- Use of shared accounts is prohibited. Where shared accounts are required, their use must be documented and approved by the respective function owner and information security officer.
- IT team must have defined process to disable/deactivate accounts that have not been accessed within a specific period of time.
- Accounts must be disabled and/or deleted in a timely manner following employment termination, according to a documented employee termination process.
- Personnel with Administrative/Special access accounts must refrain from abuse of privilege and must only perform the tasks required to complete their job function.
- Wherever possible special access accounts must be enforced with MFA or Dual authentication.
- Personnel with Administrative/Special access accounts must use the account privilege most appropriate with work being performed, abuse of access privilege is strictly prohibited.
- Privilege access to IT systems must be logged and monitored at all times. Audit log of privilege access sessions must be preserved for at least 1 year.

- Remote access to Capri Global IT systems must be made through approved remote access methods employing data encryption and multi-factor authentication.
- Remote access privilege must be terminated after a defined period of inactivity.
- Network access to production servers/services from untrusted public network must pass through Demilitarized Zone.
- Separate firewall must be configured to define DMZ from production subnet.
- Access or visibility to Capri Global's internal network IP schema should not be allowed for external network.
- Access to all IT resources including servers, firewalls, databases, wireless devices must be configured and manged according to Capri Global's "IT Systems and Operations" policy.
- Information security officer/functions is responsible for periodic review of all access and document weak configuration to production system and critical IT resources.
- Summary of access security must be shared with IT leadership team at least once in every six months.

2.11 Cloud Security

2.11.1 Overview

Cloud computing is defined by NIST as "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 is composed of five essential characteristics including on-demand self-service, broad network access, resource pooling, rapid elasticity or expansion, and measured services. It can be provided at a low level as hosted infrastructure (IaaS), at a mid-tier level as a hosted platform (PaaS), or at a high level as a software service (SaaS). Cloud service providers (CSP) can use private, public, or hybrid models.

In all term, Cloud security is essential to ensure confidentiality, integrity and availability of Capri Global Information Systems.

2.11.2 Objective

The goal of this policy is to define framework for identifying, integrating and practicing security measurements for Capri global information systems running on 3rd party cloud service providers (CSP).

2.11.3 Applicability

This policy is applicable to all individuals/unit of employee and/or vendor/contractor working with CSP/3rd party vendors for identifying, hosting or running Capri Global IT Systems on 3rd party cloud platforms.

2.11.4 Policy details

- This policy addresses all Capri Global technology, systems, data and networks implemented in private, hybrid and/or public cloud infrastructures, plus all other Capri Global IT assets implemented in cloud services as identified by Capri Global IT department.
- All other defined policies and processes of Capri Global are also applicable to Cloud workload and compliance must be ensured to maintain integrity and security of Capri Global Information systems.
- Data security must be the centre of focus and Identification/assessment of Cloud Service Providers (CSP) should be done accordingly.
- CSP must ensure that the they are compliant with a widely adopted cloud security standard that is acceptable to industry standards and regulatory requirements.

  - ISO/IEC 27017, demonstrated via certification with accreditation;
  - NIST SP 800-53, demonstrated via certification with accreditation; or
  - Level 2 of Cloud Security Alliance (CSA) Security Trust and Assurance Registry (STAR) Certification
- CSP must ensure it can demonstrate compliance with a cloud security standard by way of an annual SOC 2 Type II audit conducted by an independent third-party auditor. CSP must demonstrate compliance with security obligations if they are not covered anywhere else.
- CSP must enforce strong password policy. At minimum, it shall meet Capri Global password policy guidelines and should also have ability to enable and use multi-factor authentication for secure login.
- CSP must retain logs that are sufficiently detailed to determine who did what when for a period of 90 days online. CSP must provide online GUI access to logs.
- CSP must ensure that all underline infrastructure and services are synchronised with Stratum 1 time server.
- CSP must offer logical and verifiable separation of Capri Global IT systems and its network traffic from rest all other tenants and management traffic.
- CSP must facilitate or offer data backup and retention facilities to protect data and IT systems deployed in cloud.
- CSP must implement or offer encryption functionalities for 'data at rest' and 'data in transit'. Encryption algorithm and technology must meet latest industry standards.
- CSP shall have appropriate protection against threats and malwares. Or conduct threat & risk assessments to ensure data security of Capri Global.
- CSP shall have/offer all technical controls like WAF, firewall, IPS to prevent internet threats and protect cloud workloads.
- Capri global IT shall have approved processes and procedures to review, assess cloud security of public/private cloud.
- All existing operational controls like incident management, change management, inventory etc must be applied in Cloud operations.
- Report about major changes and incidents involving cloud security should be shared with Capri Global IT leadership team.

2.11.5 Disclaimer

While above policy tries to address known risks by applying possible controls on cloud security, some component and underline infrastructure is completely out of control for tenant owner; ensuring cloud security and protecting tenant from all possible threats is responsibility of Cloud Service Providers.

2.12 Information security awareness

2.12.1 Overview

Information security awareness is important for any organization and Capri Global isn't exception to it. "Information Security Awareness" is a formal process for educating employees about the information systems and security risks involved under Cyber security. A good security awareness program should educate employees about institutional policies and procedures for working with Company's information technology (IT).

2.12.2 Objective

The purpose of this policy is to ensure that all Capri Global employees with access to Company data, are taught Information Security Awareness in order to gain an understanding of the importance of securing the Company's data. The Capri Global seeks to establish a culture that ensures that business sensitive data is secure. This policy and associated procedures establish the minimum requirements for the Security Awareness and Training controls.

2.12.3 Policy details

- Educating users and administrators at all levels on the safe and responsible use and handling of information is necessary.
- All employees of the company must be aware of their responsibilities in protecting the data, devices and network of the company.
- Employees must be made aware of Company policies; awareness campaign must cover and educate users about Capri Global IT policies and processes.
- Capri Global IT Security function is responsible for running security awareness program for internal employees.
- Capri Global IT team shall leverage all possible methods like Desktop wallpapers, digital flyers, banners, email communications, Instant chat groups to circulate awareness contents to internal employees.
- The company shall also provide brief training to all employees after conducting gap analysis questioner that will gauge their current knowledge on security areas. Employees will then be trained by individualised programmes that will address their weakest areas first.
- Awareness campaign shall be sent out regularly, once every 4 weeks, in form of digital contents and online training courses.
- Capri Global information security officer/function has privilege and may use it to conduct surprise tests on security topics to gauge employee's knowledge of IT security areas.
- Undergoing IT security awareness program is highly recommended and all employees are expected to complete all training courses received by them within no more than 20 working days.
- If an employee has trouble accessing or completing their training, they must contact their IT support team with no undue delay.
- Failure to appear for IT security awareness training, without justifiable reasons or deliberate attempts of ignorance could lead to internal enquiry or actioned according to employee code of conduct.
- Statistic report of awareness campaigns and employee's knowledge on subject areas must be capture and published with IT leadership team.
- The security awareness training program is subject to yearly review and enhancement based on changes to the information security environment.

3 Compliance

The Information Security Officer in conjunction with the IT Operations Team will verify compliance to this policy through various methods, including but not limited to application tools reports, internal and external audits, and feedback to the InfoSec group.

Information security of Capri Global IT assets and resources is obligation of every employee, board members, external vendor resources, affiliated contractor, consultants or IT service providers. Any action by user having access to Company IT resources, which jeopardies Capri Global IT security is forbidden and shall attract appropriate action including legal proceedings.