Persistent

Acceptable Use Policy

Enterprise Information Systems

Important: The printed copy of this document is not under control

Document Control

Document No.	Document Name	Executive Summary	Revision No.	Effective from Date	Classification
PSL-ISC-POL-016	Acceptable Use Policy	This policy establishes the acceptable handling and usage of Persistent information systems by Persistent users.	6.4	02 May 2022	Internal Use Only

Authorizations

Owner	Custodian	Distribution List
EIS	EIS InfoSec & Compliance DU	Persistent Systems and Subsidiaries

Table of Contents

1. Preamble

Persistent Systems Ltd. and all its subsidiaries (collectively referred to as Persistent in this policy) employees are provided access to information systems (including hardware, software, data, connectivity and all allied assets) for conduct of business functions according to their roles. Additionally, employees are permitted to use these for limited personal work. Employees are required to make themselves aware of and adhere to all rules made for use of these systems, exercise due diligence and not take unlawful actions to disrupt or damage these systems or to disrupt others' use of the same. They are not permitted to use these systems to carry out any unlawful or malicious activities.

2. Terminology and Abbreviations

Standard terminologies used in this document

Information System	Asset/Systems in the context of this policy includes all allied assets including but not limited to: Computer equipment, e.g., servers, desktop, laptops, mobile phones, tablets, printers. Storage Media, e.g., hard drives, USB storage devices, network attached storage. Connectivity including network infrastructure, e.g., routers, firewall, telecommunications (landline and mobile networks). Software and related services including but not limited to on premise and cloud services. Data resident or processed on such information systems.
Information Media	Any device being used to store, process or transmit Persistent or customer data and/or information.
Information	Data that is (1) accurate and timely, (2) specific and organized for a purpose, (3) presented within a context that gives it meaning and relevance, and (4) can lead to an increase in understanding and decrease in uncertainty or formation of an informed opinion.
Service Owner (Includes Process Owners)	Person accountable for a specific service (Infrastructure, Application or Professional) within Persistent regardless of where the technology components or professional capabilities reside. Service owners typically belongs to EIS, but other functions/business units may be able to provide services at the enterprise level or within their function/business units.
Social Networking	A variety of applications, usually web-based, which allow users to share content, interact with each other and develop communities around similar interests. Some examples of social networking applications are Facebook, Blogger, Twitter, LinkedIn, Flickr, WhatsApp and numerous other sites.
Social Media	Social media includes any website in which visitors can publish content to a larger group. Content shared may include (but is not limited to) personal information, opinions, research, commentary, video, pictures, or business information. Examples of such

destinations include branded entities such as Facebook, Twitter, YouTube, and LinkedIn. However, blogs, special interest forums, user communities are also considered social media.

Standard abbreviations used in this document

SIRT	Security Incident Response Team
ISMS	Information Security Management Systems
EIS	Enterprise Information Systems
ERP	Enterprise Resource Planning
VM	Virtual Machine

3. Scope

This policy is applicable across all Persistent facilities for all employees, contractors and third parties handling or working with Persistent information and/or information systems.

4. Objective

The objective of this policy is to outline the acceptable use of all Persistent information and information systems. Persistent, being a software engineering and services company, operates in a complex information systems environment, including various types of hardware, software and connectivity to carry out its business. To ensure security and business continuity, it is necessary that all access to such systems is regulated and monitored. Every user of these systems has a role to play in ensuring these objectives.

5. References and ISO/IEC Controls Addressed

5.1. References

- Information Security Policy
- Access Control Policy
- Information Media Handling Procedure
- Password Policy
- Data Governance Policy

5.2. ISO/IEC 27001 Controls Addressed

- A.8.1.3 - Acceptable use of assets

6. Roles and Responsibility

Role	Responsibility
All Users	a) Understand and adhere to the Acceptable Use Policy
Service Owner(s)	a) Implement and maintain the information systems and media b) Ensure that controls are implemented as per the security policy requirements
EIS InfoSec & Compliance	a) Establish the security controls requirements b) Investigate reported non-compliance c) Raise SIRT in cases of confirmed non-compliance. d) Provisioning of exception to Password Policy clauses to the users.
People Management	a) Initiate action against the employee if any non-compliance adhered. b) Ensure policy signoff at the time of onboarding & maintain record in ERP.
EIS	a) Provisioning of social media websites to all users. b) Blocking of websites which are malicious or based on reputation of the websites or requests.

7. Policy

7.1. General Use and Ownership

a) Persistent proprietary information stored on physical media and electronic and computing devices, whether owned or leased by Persistent, the employee or a third party, remains the sole property of Persistent. You must ensure through legal or technical means that proprietary information is protected in accordance with the Data Governance Policy.

b) All employees have a responsibility to report the theft, loss or unauthorized disclosure of Persistent proprietary information or asset under the user's control or that is brought to your notice.

c) Users may access, use or share Persistent proprietary information only to the extent it is authorized and necessary to fulfill the user's assigned role.

d) Employees are responsible while using the information for personal use & due rationality must be exercised. If there is any uncertainty, employees shall consult their respective managers and EIS InfoSec & Compliance team. Employees shall not retain any non-corporate personal data such as personal photographs, medical reports, family documents etc. on corporate information assets allocated to them.

e) For security and network maintenance purposes, authorized individuals within Persistent may monitor and audit information systems.

f) Persistent Information Systems have users in privileged access roles who have access beyond regular workflows. Such access needs to be used for no other

purpose or role other than for service management or system administration or for that specific purpose for which access was provided to such user.

7.2. Security and Proprietary Information

a) All users shall not use non-Persistent information systems to process, handle, store or manage persistent information unless specifically authorized.
b) All users are responsible to secure the credentials provided to them and should not share these with anyone. System level passwords and user level passwords should be changed as per password policy unless an exception is authorized by the InfoSec team.
c) Before attempting to give access to Persistent Information systems, Service owners need to ensure and confirm that they have adequate authority to grant such access and a clear record of granting as well as revoking of such access shall be maintained. End users should be aware that all such access is subject to audit and regulatory requirements. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
d) Service owners should ensure that ownership and access are enforced as granularly as possible using all technical means at their disposal.
e) There may be situations where Persistent users are required to share information with people outside Persistent or to provide access to resources to Non-Persistent entities. Such access needs to be properly circumscribed and supported by all required approvals. In general, all access to non-persistent entities needs to be cleared by InfoSec & compliance.

7.3. Inadvertent Access

Malicious agent/intruders can gain access to Persistent information and information systems through errors committed by authorized/privileged users. The following should be ensured to prevent the same:

a) Any information that the user consider sensitive or vulnerable should be password protected, where possible or it should be encrypted.
b) All users must lock the screen or log off when the device is unattended.
c) Employees must use extreme caution when opening e-mail with attachments or links which they received from unknown senders, which may contain malware.

7.4. Software Installation and Compliance

a) In general, software may only be installed on specific hardware/Virtual machine for which specific permission has been provided.
b) Installation of personal (licensed/procured/freeware/shareware) software is prohibited.
c) Any planned software installation must be communicated to Software Compliance team, along with business justification and business manager approval, for reviewing the license terms. Software may only be installed on positive confirmation or by automated installation using Persistent software repositories.

7.5. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during their legitimate job responsibilities.

a) Under no circumstances is an employee authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Persistent Information Systems and Persistent/customer owned resources.

7.5.1. Use of Corporate Endpoints

a) Users are advised that the PSL provided asset(individually allocated, project allocated or otherwise) including VMs, Cloud, Servers, Laptops, Desktops or any other device having compliance requirements must be connected to the PSL intranet/ Internet at least for one full day in a week. This is a mandatory requirement of compliance and failure to adhere to the same may call for strict actions as per SIRT policy.
b) Users are advised to ensure that post exit from a project, they need to ensure to remove all project sensitive & customer confidential data from their user endpoint and/or personal backups. It is expected that such data will be handed over to project manager in case it needs to be retained. Such data shall be held in project repositories.

7.5.2. System and Network Activities

The following activities are strictly prohibited, with no exceptions:

a) Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Persistent.
b) Unauthorized copying of copyrighted material, downloading / distributing / storage of pornography, MP3, audio, video, games etc. is not acceptable.
c) Downloading/installing/using freeware/shareware or any software tools which is of non-business in nature and not approved by the business is prohibited.
d) Revealing your corporate credentials to others or allowing use of your credentials by others. This includes family and other household members when work is being done at home is prohibited.
e) Sharing company/official information, Persistent employee personal information (such as providing information about, phone numbers of, or lists of, Persistent employees) to parties outside Persistent Systems or customer provided information with unauthorized personnel within or outside of company be strictly prohibited. Any employee found guilty of such an offence shall be subjected to suitable disciplinary action as per the company policy.
f) Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

g) Using a Persistent information system to actively engage in procuring or transmitting material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, defamatory or otherwise inappropriate or unlawful.
h) Tampering, disengaging or otherwise circumventing information systems security controls.
i) Making fraudulent offers of products, items, or services originating from any Persistent's account.
j) Connecting devices to Persistent infrastructure, without prior notification and consent of EIS and InfoSec teams against a valid business justification and approval by manager at laid down level.
k) Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
l) Port scanning or security scanning is expressly prohibited unless prior notification to EIS and InfoSec is made, and the activity is authorized by InfoSec & Compliance DU.
m) Executing any form of network monitoring which shall intercept data not intended for the employee's host unless this activity is a part of the employee's normal job/duty.
n) Circumventing user authentication or security of any host, network or account.
o) Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
p) Introducing honeypots, honey nets, or similar technology on Persistent information systems
q) Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session via any means, locally or via the Internet/Intranet/Extranet.
r) Providing unauthorized third parties, including family and friends, access to the Persistent information systems, resources or facilities
s) Access - Users are required to be aware of locking and access restriction mechanisms. Users are responsible to secure and maintain integrity of account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e., Smartcard), or similar information or devices used for identification and authorization purposes. Users shall not share any of the identification and authorization methods with others.
t) Cloud Computing and Storage
    i. Persistent Users may not store Persistent data on any non-Persistent approved storage sites.

ii. Personal cloud services accounts must not be used for the storage, manipulation or exchange of Persistent-related communications or Persistent-owned data

7.5.3. Use of Personal Computing Endpoints to connect to Persistent Information Systems

a) As per Persistent's policies, company owned assets are provided for all business use. Use of Personal endpoints is not authorized for any business use or to connect to any business or persistent information asset.
b) Connecting/usage of unauthorized personal devices is strictly prohibited under this policy

7.5.4. Email and Communications Activities

When using Persistent information systems, users must realize that they represent the company. Whenever employees state an affiliation to Persistent, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". The following activities are strictly prohibited, with no exceptions:

a) Sending unsolicited email messages, including the sending of "junk mail", chain mails or other advertising material to individuals who did not specifically request such material (email spam).
b) Any form of harassment via email or telephone.
c) Unauthorized use, or forging, of email header information.
d) Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass.
e) Sharing personal information, sensitive or confidential information owned by Persistent or its customer, with unauthorized users.
f) Usage of corporate email to subscribe to non-business services.
g) Connecting to commercial email systems (e.g., Gmail, Hotmail, Yahoo) without prior management approval. Users must recognize the inherent risk in using commercial email services as email is often used to distribute malware.

7.5.5. Photography

a) Photography is in general forbidden within all Persistent facilities except for atrium, cafeteria and the courtyard. Inadvertent loss of information can happen through photos of screens or documents with data on them.
b) Photos of structure and layout of Persistent controlled workspaces, whether office, admin or security facilities is Persistent Confidential information and the standard rules of dealing with such information will apply.
c) Valid business approval is needed for photography to be permitted within premises for business reasons. In such a case user must ensure
    i. Photos cannot cover any computer screen/whiteboard/ projection screen with Persistent data and/or customer data on it.
    ii. Camera must be registered with security.

iii. All photos taken in prohibited areas need to be deleted from camera and need to be held and reviewed by business approver. The approver must ensure any photography must comply with all provisions in this policy

7.5.6. Use of Social Media

a) Blogging and social media usage, whether using Persistent information systems or personal computer systems, is also subject to terms and restrictions set forth in this policy. Your personal blogging and social media usage should not violate Persistent policies, not be detrimental to Persistent's best interests and should not interfere with regular work duties of Persistent personnel.

b) Do not use the same passwords for social media that you use to access Persistent Information Systems and computing resources.

c) Users are prohibited from revealing or using any Persistent confidential or proprietary information, trade secrets or any other material covered by Persistent policies when engaged in blogging or social media. Do not comment on Persistent stock price or confidential financial information such as future business performance or business plans. Do not register accounts using the Persistent brand name or any other unregistered or registered trademarks.

d) Do not conduct confidential business with a customer or partner business through your personal or other social media.

e) You are responsible for all content posted and activity that occurs under your account on social media and blogs and Persistent will not be liable for any loss or damage through any social media.

f) Employees shall not engage in any blogging or social media that may harm or tarnish the image, reputation and/or goodwill of Persistent Systems and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or on social media or otherwise engaging in any conduct prohibited by Persistent Systems policies. Do not use ethnic slurs, personal insults, obscenity, or engage in any conduct that would not be acceptable in the Persistent workplace. You should also show proper consideration for others' privacy and for topics that may be considered objectionable or inflammatory.

g) Employees may also not attribute personal statements, opinions or beliefs to Persistent Systems when engaged in blogging or social media. If an employee is expressing his or her beliefs and/or opinions in blogs or social media, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Persistent Systems. Employees assume all risk associated with blogging and social media.

h) Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, Persistent Systems' trademarks, logos and any other Persistent Systems intellectual property may also not be used in connection with any blogging or social media activity. You are sole responsible for any cybercrime reported against you through any social media even when you are

using it through Persistent information systems. Persistent will not entertain any such reports and will not be responsible for the same.

7.5.7. Personal Use of Social media activities

It is understood that some individuals performing work on behalf of Persistent will be active on social media. Do adhere to the below points.

a) Access to social media must be confined to limited personal use. Ensure that your actions do not violate Persistent acceptable usage and other ISMS policies.
b) Do not use your corporate email ID on any non-Persistent website. It may only be used if it is in pursuance of your professional role. Further, you are required to ensure that the password linked to your ID within Persistent's system is never used on any public websites, with or without your Persistent ID.
c) If you are discussing products or services provided by Persistent Systems or any of its subsidiaries, you must identify yourself as on employee and make it clear that the views are yours and do not represent the views of Persistent Systems.
d) You must not speak disparagingly about persistent systems, its employees or officers, or any product or service provided by Persistent Systems.
e) You should show proper consideration for others' privacy and for topics that may be considered objectionable or provocative. Do not use ethnic slurs, personal insults, obscenity, or engage in any conduct that would be against the Code of Conduct policy of Persistent.
f) You are responsible for all content posted, liked or shared and activity that occurs under your account. Persistent will not be liable for any loss, damage or issues arising through usage of any social media by individuals.
g) You are solely responsible for any cybercrime reported against you through usage of any social media using Persistent network.
h) Do not register accounts using the Persistent brand name or any other unregistered or registered trademarks.
i) Do be professional. If you have identified yourself as a Persistent Systems employee within a social website, you are connected to your colleagues, managers and even Persistent Systems customers. You should ensure that content associated with you is consistent with your work at Persistent Systems.

7.5.8. Guest Wireless

a) Guest wireless account is provided for at various Persistent facilities for accessing internet from Persistent premises for visitors, customers, auditors and others who are not Persistent personnel.
b) Persistent personnel are not allowed to create guest user account for their own use through Persistent laptops or mobile devices.

7.5.9. Privacy

a) All users retain the right of privacy in their personal data if they are using the Persistent Information resources in a manner consistent with this Policy. Likewise,

users are obligated to respect the right of privacy that other users have in their own data.

b) Users should note that the Persistent, in emergency situations, may also require backup and caching of various portions of Information Systems; logging of activity; monitoring of general usage; and other activities that are not directed against any individual user, for the purposes of emergency maintenance or restoring normal operations of the Information Systems.

7.5.10. Malware and Online Crime Prevention

Social media is commonly used by the online criminal community to deliver malware and carry out schemes designed to damage property or steal confidential information. To minimize risk related to such threats you need to adhere to the following guidelines.

a) Do not use the same passwords for social media that you use to access company computing resources.

b) Do not click on the links or download software from social media pages as they may redirect you to malicious websites. Visit the necessary websites by typing the URL.

c) If any content you find on any social media Web page looks suspicious in any way, close your browser and do not return to that page.

d) Configure social media accounts to encrypt sessions whenever possible. Facebook, Twitter and others support encryption as an option. This is extremely important for roaming users.

7.5.11. Speaking on behalf of Persistent

a) Employees are not allowed to disclose information that are financial, operational and legal in nature, as well as any information that pertains to customers. Desist from talking about financial information, sales trends, strategies, forecasts, legal issues, future promotional activities on social media.

b) Employees are not allowed to give out personal information about customers or employees, posting confidential or non-public information. Responding to an offensive or negative post by a customer.

c) Do not induce in any business association with a customer or partner through social media platforms.

d) Do ask for permission to publish or report conversations that are meant to be private, confidential or internal to Persistent and when in doubt, always ask permission from respective managers, Persistent InfoSec & Compliance team or Legal department. Do use your best judgement based on the data that is being published.

e) Do not disclose or use Persistent confidential or proprietary information or that of any other person or company on social media websites.

f) Do not cite or reference customers, partners or suppliers without their written approval.

8. Enforcement and Compliance

Violations of Persistent Acceptable Use Policy or any other security policy or regulation will be subject to investigation by InfoSec team and may lead to revocation of access to Persistent information system and network privileges as well as other disciplinary actions as decided by SIRT and appropriate external law enforcement authorities, as applicable, which may lead to termination.

9. Review

This policy shall be reviewed at least annually, and updated per the new risks identified, the mitigation controls required and the business requirement.

10. Exception Handling

Situations in which the requirements outlined in this Policy cannot be adhered to, must be documented and formally approved by InfoSec. However, Operational implementation will be the respective Service Owner's responsibility.

10.1. Due diligence for new exceptions

a) Every type of exception handling will be reviewed & proposed by the Service Owners & approved by InfoSec.
b) For each exception, a risk assessment must be performed. For identified risks possible compensating controls need to be analyzed and identified.
c) Compensating controls must be implemented to mitigate the risks that exist.

10.2. Maintenance of Records

a) Exceptions shall be provided to for a specific project and for a specific time. At the end of the tenure or project or transfer of the employee to another project the exception shall be revoked.
b) Operational records of all exceptions will be maintained as a service request by the respective Service Owners.
c) Every such service request must record
    i. The nature of the exception
    ii. A reasonable explanation for why the policy exception is required
    iii. Any risks created by the policy exception
    iv. Evidence of approval by InfoSec for the type of service request
d) Upon expiry of exception duration, it is the responsibility of the service owner to deprovision such an exception. A record of such deprovisioning must be made available for audit or review.

10.3. Exception Review:

a) Registered exceptions must be reviewed annually by the service owners to assess if compensating controls still mitigate the risk or if the motivations for accepting the risk are still valid.

b) In case of new controls being implemented by service owners which mitigate the need for exception, service owners will obtain sign-off from InfoSec before implementation of such controls.

11. Contact for Queries

Please contact EIS-Governance in case of any additional queries.

12. Version Control

Date	Ver	Description	Prepared By	Reviewed By	Authorized By
29 Mar 2007	Initial	Draft of Acceptable use of persistent assets policy	ISM Group		
10 Aug 2007	1.1	Reviewed the Acceptable use of Persistent Assets Policy	ISM Group	Head Information Security (Deepak Bhandarkar)	Head Information Security (Deepak Bhandarkar)
24 Aug 2007	1.2	Revised the acceptable use of Persistent Asset policy	ISM Group	COO (Srikanth Sundararajan)	COO (Srikanth Sundararajan)
4 Dec 2008	1.3	Renamed and Revised Acceptable Use Policy	ISM Group	Srikanth Sundararajan	Srikanth Sundararajan
3 Dec 2010	1.4	Added Asset Owner and Software compliance details	ISM Group	COO (Nitin Kulkarni)	COO (Nitin Kulkarni)
30 Nov 2011	1.5	Modified as per the new template and reviewed the policy	InfoSec	Mohit Bhishikar (Head IT and InfoSec)	Mohit Bhishikar (Head IT and InfoSec)
1 Jan 2013	2	Updated as per the new template and reviewed the policy.	InfoSec team	Nikhil Gadgil	Mohit Bhishikar, Head – Persistent IT
27 Dec 2013	2.1	Revised Inclusion of DLP agent requirement on laptops	Shweta Rana	Mrunmayi Kulkarni Manager – InfoSec team	Mohit Bhishikar Head – Persistent IT
5 Mar 2015	3.0	Revised Inclusion of social media policy	Kumar Madnendu	Mitasha Pujari	Mrunmayi Kulkarni Manager – InfoSec team
18 Aug 2015	3.1	Inclusion of guest wireless security points	Mitasha Pujari	Sachin Belsize	Mrunmayi Kulkarni Manager – InfoSec team
1 Feb 2016	3.2	Formatting level changes	Ashish Gargote	Mitasha Pujari	Mrunmayi Kulkarni Manager – InfoSec team

17 Feb 2016	3.3	Include asset recovery from PSI exit cases	Anuja Kanhere- People Management	Nidhi Mulik – People Management	Mrunmayi Kulkarni Manager – InfoSec team
15 Jun 2016	3.4	Reviewed: No Change	Ashish Gargote	Mrunmayi Kulkarni Manager – InfoSec team	Mrunmayi Kulkarni Manager – InfoSec team
13 Sep 2016	3.5	Reviewed – Change in approval hierarchy	Mitasha Pujari	Mrunmayi Kulkarni	Mohit Bhishikar - CIO
10 Oct 2017	4.0	Reviewed – Updated document, removed Persistent Assets, updated Structure, updated Roles to reflect change in org structure.	Amey Kantak (Senior Team Lead EIS-Governance) Kantak	Avinash D (Deputy General Manager) Vaibhav Shende (Asst. Manager – Legal) Pratyush P (Asst. Manager – Business Development)	Amarjit Singh Head – EIS
27 Dec 2018	5.0	Merged –Social Media Usage Policy and Internet Usage Policy Added - Guidance on Use of personal computing endpoints to connect to Persistent Information systems and cloud guidance Document ID updated from PSL-IS-PL-024 to PSL-ISC-POL-016	Amey K (Lead – EIS Risk & Governance)	Avinash D (Head- InfoSec & Compliance DU)	Amarjit Singh (Head – EIS)
23 Dec 2019	6.0	Reviewed, Template updated	Amey K (Manager – EIS Risk & Governance)	Avinash D (CISO)	Amarjit Singh (CIO)
15 Apr 2019	6.1	Policy reviewed. Exception Handling Section added.	Amey K (Manager – EIS Risk & Governance) Pranav Goyal (Sr. InfoSec Analyst)	Avinash D (CISO)	Amarjit Singh (CIO)

02 Jul 2020	6.2	Policy reviewed with respective service owners. No changes made.	Rama M (Lead-Risk & Governance), Keyura Mujumdar (Analyst – Risk & Governance)	Paresh V (Engineering Lead), Girish Atre (Lead-People Services), Meena B (Engineering Manager), Akshay A (Manager - IT Portfolio), Amey K (Manager - Risk & Governance)	Avinash D – (CISO)
14 Apr 2021	6.3	Compliance requirements by end users for corporate assets added Guidance barring use of personal assets for official use added	Rama M (Asst Manager – Risk & Governance)	Amey K (Manager - Risk & Governance)	Avinash D – (CISO)
02 May 2022	6.4	Updated guidance for personal data handling for employees	Mridul M (InfoSec Analyst – Risk and Governance) Rama M (Associate Manager – Risk & Governance)	Amey K (Sr. Manager - Risk & Governance)	Avinash D – (CISO)