Acceptable Use Policy, PO-10-3-12-0-LUX-(ENG)

Quality Management System

Exported on 08/24/2023

Table of Contents

1. Purpose

The purpose of this policy is to govern the business and personal use of Luxoft Information Systems and Luxoft Owned Devices and to establish the controls and responsibilities to meet the requirements in this policy.

This policy defines Luxoft requirements for addressing security, reputational, and legal risks associated with the use of Luxoft Information Systems and Luxoft Owned Devices to prevent breaches of contract, the loss or unauthorized disclosure of any confidential or otherwise sensitive data of Luxoft, its employees, customers, suppliers, or business partners, and violations of Luxoft policy and applicable laws.

2. Scope

This policy applies to:

- Luxoft Information
- Luxoft Information Systems
- Luxoft Owned Devices
- Covered Persons

3. Definitions

Covered Persons	Any Luxoft Employee and/or Luxoft Third Party as defined in this policy.
Covered Systems	Any Luxoft Information System(s) and any Luxoft Owned Devices as defined in this policy.
Luxoft Employee	Any employee or worker of Luxoft, including any director, officer, or intern.
Luxoft Information	All Luxoft, customer, supplier, employee, and other third party confidential, proprietary, financial, personal, or other sensitive information stored, transmitted, or received using a Covered System whose unauthorized disclosure or access can result in harm to Luxoft, a Luxoft Customer, or a third party to whom that information belongs. The term “Information” applies regardless of whether the Information exists in digital, audio, electronic, facsimile, or other form.
Luxoft Information Owners	For the purposes of this policy means Luxoft management, heads of business units and departments.
Luxoft Information System(s)	Any communication or information system owned or controlled by Luxoft and used to collect, store, transmit or receive, share, disclose, delete or otherwise process (“**Use**”) Covered Luxoft Information. It also means any customer communication or information systems or acquired services to the extent such information systems or services are physically or logically connected to Luxoft Information Systems or owned, controlled, managed, or supervised by Luxoft.
Luxoft Owned Device(s)	Any Luxoft provided device which could include mobile phones, laptops, tablets, notebooks, personal computers (PC), and any other portable or desktop computer systems, whereby the device or a compartment of the device, is owned, controlled, managed, or supervised by Luxoft.

Personal Devices	Any device owned by Covered Persons which could include mobile phones, laptops, tablets, notebooks, personal computers (PC), and any other portable or desktop computer systems, whereby the device or a compartment of the device, is owned by Covered Persons and not controlled, managed, or supervised by Luxoft.
Luxoft Third Party	Any business partner, supplier, consultant, contractor, sub-contractor, agency or agency worker, reseller, distributor, joint venture, consortium, teaming partner, channel partner, lobbyist, law firm, or other business partner that will either assist Luxoft in delivering services, represent Luxoft's interests to a customer or third party, or provide Luxoft a service.
Luxoft	For purposes of this policy, means Luxoft Company, its parents, subsidiaries, affiliates, and inherited businesses.
Use	Collecting, storing, transmitting, receiving, sharing, disclosing, deleting, or otherwise processing the relevant data, information, or subject matter.

4. Requirements

>> 4.1 Bring your own device (BYOD)

DXC Luxoft employees are only allowed to access the following company resources from personal laptops/PCs for the purposes explicitly mentioned below:

- Only the web version of Outlook to send/receive e-mails and manage the calendars
- Only the web version of Teams to exchange messages with other company employees and participate in meetings
- MyHome to submit sick leaves, vacation requests, track MyTasks/SD requests
- Service Desk to submit and track requests
- LuxStaff to submit sick leaves, vacation requests, check information on employee's own profile
- TRM to submit timesheets
- LuxTalent to pass trainings, submit training requests, goals

Personal laptops/PCs used to access the company resources above must meet all the following security requirements:

- Up-to-date antivirus
- Up-to-date OS
- Must be password protected
- Not publicly accessible

Use of personal laptops/PCs to access DXC Luxoft/Client data for purposes other than those mentioned above is prohibited.

It is prohibited to install DXC Luxoft software on personal laptop/PC.

It is prohibited to install Client software on personal laptop/PC. Unless it is explicitly stated in the contract with the Client.

It is prohibited to download, store or process DXC Luxoft/Client data on a personal laptop/PC.

It is prohibited to enroll a personal laptop/PC into DXC Luxoft domain/Intune.

>> 4.2 Acceptable Use

Luxoft provides Covered Systems to Covered Persons for legitimate business purposes. Covered Persons are expected to exercise good judgment and professionalism when using any Covered Systems. Any use of a Covered System must be in accordance with this policy and in support of Luxoft business purposes.

A Covered Persons' relationship with Luxoft is one based on trust, which must be maintained at all times. Covered Persons must always hold themselves to the highest standards of conduct to maintain Luxoft's reputation and the integrity of Luxoft's business.

Incidental and occasional personal use of a Covered System is allowed providing such use complies with the requirements of this policy and other applicable policies, does not interfere with workplace productivity or Luxoft's systems or business operations, does not conflict with any Luxoft business activity, does not consume more than a trivial amount of Luxoft's resources, and is lawful.

Luxoft Information and Covered Systems must be handled in accordance with the Rules on Company Information Treatment by Employees.

Covered Persons should use Luxoft owned PCs/laptops enrolled into corporate Intune and/or Client-provided machines to access, transfer, store, or process Luxoft Information.

Covered Persons should be aware that all use of Covered Systems is subject to monitoring as described in this policy and related policies. As such, Covered Persons have no right to, nor expectation of, privacy with respect to their use of the Covered Systems (subject to applicable laws). Covered Persons are required to cooperate with any investigation into a suspected breach, which may involve providing Luxoft with access to the relevant Covered Systems and any relevant passwords and login details.

>> 4.3 Unacceptable Use

Use of personal devices to access, transfer, store, or process Luxoft Information is prohibited.

Covered Persons are not permitted to use any Covered Systems to view, listen to, access, amend, update, change, or use any Luxoft Information without proper authorization. Covered Persons are also not permitted to use any Covered System in any way or for any purpose which:

- is or likely to be unlawful
- is or likely to be harmful to or interferes with the use of the Covered System
- infringes intellectual property rights
- results in the publication of threatening, offensive, discriminatory, or derogatory material
- constitutes spam/email abuse, a security risk, or a violation of privacy
- constitutes a violation of Luxoft policies

Examples of unacceptable use of Covered System include, but are not limited to:

>> 4.3.1 Unlawful activities:

- using Luxoft resources in a manner that violates Luxoft policies and applicable laws, including, without limitation, those laws relating to discrimination and harassment, privacy, confidentiality, financial disclosure, intellectual property and proprietary information, defamation, and criminal laws
- accessing, promoting or any other activity otherwise involving internet sites for gambling or any illegal activity
- is otherwise illegal or solicits conduct that is illegal under laws applicable to Covered Persons or to Luxoft

>> 4.3.2 Infringement of intellectual property rights:

- downloading, storing, playing, or transmitting material that infringes any copyright, trademark, or other proprietary right
- circumventing or assisting others in defeating technical copyright protections
- downloading or distributing pirated software or data
- installing or using peer-to-peer file-sharing programs or accessing those types of networks

>> 4.3.3 Offensive content:

- publishing, sharing, playing, listening to, accessing, printing, downloading, or viewing (or any other similar action) any offensive content or links to any offensive content that we reasonably believe fall within any of the following categories:
  Obscene content: Content that constitutes, depicts, fosters, promotes, or relates in any content manner to all forms and types of pornography including bestiality, non-consensual sex acts, or material that is offensive to accepted standards of morality or decency.
  Libel and slander: Content that we reasonably believe is false or defamatory in relation to any legal person (including any individual, whether colleague, customer, or vendor, or any company or other body corporate) or violates the privacy of any natural person.
  Threatening and abusive content: Content that (a) is excessively violent, gratuitously violent, incites violence, threatens violence, or contains harassing content or hate speech; or (b) creates a risk to a person's safety or health, creates a risk to public safety or health, compromises national security, or interferes with an investigation by law enforcement.
  Discriminatory content: Content that is discriminatory, offensive, derogatory, or may cause embarrassment to others, including material which breaches our Corporate Code of Conduct.
  Other: Any other content that is otherwise malicious, fraudulent, or may result in retaliation against Luxoft by offended viewers or recipients, or is intended to harass or threaten, or which is likely to create any criminal or civil liability for you or Luxoft.

>> 4.3.4 Spam/email abuse:

- sending unsolicited email or bulk mail
- using any false, misleading, or deceptive TCP-IP packet header information in an email or a newsgroup posting
- publishing any content which is unfair or deceptive under the consumer protection laws of any jurisdiction, including chain letters and pyramid schemes
- interfering with service to any user of the Covered System or other network including, without limitation, mail bombing, flooding, deliberate attempts to overload a system, and broadcast attacks

>> 4.3.5 Security risk or violations:

- distributing malicious or unauthorized software that covertly gathers or transmits information about a user
- performing any unauthorized scanning or information gathering regarding the Covered System, including the following: port scanning, security scanning, network sniffing, keystroke logging, or other information gathering techniques

- posting or transmitting proprietary or Luxoft Information related to clients, suppliers, vendors, allied parties, or other third parties without express authorization
- gaining unauthorized access to or use of data, systems or networks, including any attempt to probe, scan, or test the vulnerability of a system or network or to breach security or authentication measures without express authorization of the owner of the system or network
- monitoring data or traffic on any network or system without the express authorization of the owner of the system or network
- deliberately propagating a virus, malware, or any other malicious program code
- engaging in behavior that results in any server being the target of a denial-of-service attack (DoS)
- performing any conduct that is likely to result in retaliation against Luxoft or Luxoft's employees, officers, or other agents

>> 4.3.6 Unauthorized use:

- soliciting or recruiting for any non-job-related commercial ventures, religious or political causes, outside organizations, or other non-job-related solicitations
- downloading entertainment software or games, or to play games over the internet unless with express authorization
- to embarrass Luxoft Employees, or to jeopardize Luxoft's reputation
- any act which improperly exposes trade secrets or other confidential or proprietary information of Luxoft or another person
- posting or storing Luxoft Information on public storage sites
- engaging in activities for personal gain or a personal business, or for any commercial or business purposes other than Luxoft's purposes unless with express authorization (e.g., cryptocurrency mining, online gambling, etc.).

>> 4.4. Monitoring

All Luxoft Information belongs to Luxoft Company, regardless of who owns the device on which the Luxoft Information is created on, transmitted to, received or printed from, or stored or recorded on or otherwise used.

Luxoft reserves the right to monitor, intercept, and review, in accordance with applicable law, all employee activities using the Covered Systems, including the Use of Luxoft Information to ensure that Luxoft rules and policies are being complied with and for legitimate business purposes.

Covered Persons are advised not to use the Covered Systems for any personal matter intended to be kept private or confidential and Covered Persons should have no expectation of privacy in any data on a Covered System. If Covered Persons use the Covered System to process personal data about non-business related third parties (for example family and friends), Covered Persons should be aware that this may be inadvertently monitored, intercepted, reviewed, or erased. Covered Persons should ensure that any non-business related third parties are aware that their personal data may be inadvertently monitored.

>> 4.5 Security and Confidentiality

When accessing or using Luxoft Information or Covered Systems, all Covered Persons must adhere strictly with the information security requirements of Luxoft as updated from time to time. This includes, but is not limited to, Rules on Company Information Treatment by employees and other policies and standards published on the Corporate QMS portal. In the event of a lost or stolen Luxoft Owned Device, inappropriate access of a Covered System, or where a staff member believes that a Luxoft owned Device or a

Covered System may have been accessed by an unauthorized person or otherwise compromised, the staff member must report the incident to Luxoft Security Incident Response Team lux-incident-report@dxc.com immediately.

5. Responsibilities

Luxoft Employees who violate or attempt to violate this policy may be barred from continued use/access to Covered Systems and may be subject to disciplinary action, up to and including termination of employment.

Luxoft Third Parties who violate this policy may be barred from continued Use of/access to Covered Systems.

Covered Persons must also immediately notify Luxoft's Security Incident Response Team at lux-incident-report@dxc.com of any suspected breach of this policy and cooperate fully in any investigation in relation to any actual or suspected breach of this policy. Please note that misuse of Covered Systems and/or of the internet may also, in some cases, be a criminal offence.

Where evidence of any failure to comply with or violation of this policy is suspected or identified, we may undertake a more detailed investigation which may include disclosure of information pertaining to any suspected or identified misuse to (i) those authorized to conduct the investigation, (ii) any witnesses or managers involved in any such investigation and (iii) the police or regulatory authorities.

6. List of changes

№	Approval date	Version	Subject of change	Issued/Checked by
1	17.10.2022	1.0	Policy creation	Muzaffar Sheraliev
2	12.06.2023	1.1	Point 4 updated	Maslova, Ayna
3	03.08.2023	1.2	Point 4 updated, Point 4.1 (BYOD) was added (SD2695723)	Maslova, Ayna
4	08.08.2023	1.3	Point 4.1 (BYOD) was updated(SD2695723)	Maslova, Ayna