Rules on Company information treatment by employees, PO-10-3-05-0-LUX-(ENG)

Quality Management System

Exported on 08/24/2023

Table of Contents

Purpose

The present rules describe internal regulation of information protection which shall be followed by Company’s employees.

Scope

This policy applies to:

- Company Information
- Company Information Systems
- Covered Persons

Definitions

Covered Persons means any Company Employee and/or Company Third Party as defined in this policy.

Company Employee means any employee or worker of Luxoft, including any director, officer, or intern.

Company Third Party means 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.

Company Information means 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.

Company Information System(s) means 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.

Use means collecting, storing, transmitting, receiving, sharing, disclosing, deleting, or otherwise processing the relevant data, information, or subject matter.

1. Information Categorization

Protection of information, received by Covered persons during their ordinary duty performance – is a set of means of providing Covered persons with access to information to execute their duties and prevent the access to information of third parties or Company's employees if it is not connected with their duty execution.

The present rules describe internal regulation of information protection which shall be followed by Covered persons. If information can be referred to commercial or official secret according to the current legislation and internal Company's statements (Rules on documents treatment, presenting a commercial secret), there are rules determined by legislation and this Statute.

All Covered Persons are expected to know the information classification level of the information they use as part of their job function.
All Covered Persons are expected to use their knowledge of the context and business value of the data they create and handle, so that informed decisions can be made about how it is managed, protected, shared and categorized.

The activities dealt with treatment and protection of information are carried out by CSO.

In this context "information" is understood as any official information (categories 2, 3, and 4 according to adduced classification).

>> #1.1 Public information

Non-Sensitive Unmarked Information, the compromise of which is not expected to cause damage to Company's business activities or competitive status, and therefore may be suitable for public dissemination, if appropriate; or information obtained from the public domain.

Examples of Public information:

- Publicly issued annual report
- Press releases
- Advertisements
- Publicly issued financial results
- Publicly issued position descriptions
- Content of public Internet sites
- Articles in mass media

>> #1.2. Company-wide information

Low Sensitivity Information, the compromise of which could cause damage to Company's business activities or competitive status and, therefore, warrants careful consideration before sharing, as well as protection from unauthorized modification and disclosure.

Intended for access and use by all Company employees but is not to be disclosed outside of Company.

Examples of Company-wide information:

- Corporate policies and procedures
- General information on projects
- Employee broadcast announcements
- Internal positions descriptions not altered for public distribution
- Information deemed suitable for release to prospective new clients not yet covered by a non-disclosure agreement (NDA)

>> #1.3. Internal use Information

Medium Sensitivity information, the compromise of which could be expected to cause significant damage to Company's business activities or competitive status and justifies heightened protective measures to protect it against intended or accidental loss, attack or unauthorized access.

Information of restricted access, generally access and used by all employees of a particular department or project.

Examples of Internal use Information:

- Client contracts and deliverables
- Approaches or proposals
- Compensation range tables
- Department-level regulations
- Project documentation

>> #1.4. Confidential Information

High sensitivity information, the compromise of which could be expected to cause catastrophic damage to Company's business activities or competitive status, requiring the highest levels of protection from intended or accidental loss, attack or unauthorized access.

Accessed by a small group of highly trusted persons with additional security measures applied to prevent disclosure.

Examples of Confidential Information:

- Financial information
- Corporate financial forecasts or information used to produce such forecasts, or which may impact them
- Financial results prior to public release
- Non-public financial information including test results and conclusions from management's SOX testing
- Personally identifiable information (PII) of employees or customers

- Pricing or marketing strategies
- Company plans
- Materials of management meetings
- Salary and bonuses information
- Mergers and Acquisitions information
- Product development plans
- Intellectual property that supports a critical business strategy (trade secrets)
- Confidential legal advice
- Sensitive strategic or workforce restructuring information yet to be made public, which may have positive or negative impact on Company financial reporting, strategy or credibility

2. Information labeling and handling

Information must only be made accessible to the authorized group of persons. This is only permissible in the scope of the tasks agreed on and with compliance to existing regulations. The "Need to know" principle must be applied. Information must be protected against access by unauthorized persons according to its current confidentiality classification during the entire life cycle.

The following regulations apply:

#	Confidentiality level	Labeling	Access Management	Disclosure	Data Storage	Data Transfer	Data Deletion&Disposal
1	**Public**	None	**Hard copies:** No restrictions **Soft copies:** No restrictions	No restrictions	**Hard copies:** No restrictions **Soft copies:** No restrictions	**Hard copies:** No restrictions **Soft copies:** No restrictions	**Hard copies:** No restrictions **Soft copies:** No restrictions
2	**Company-wide**	Mark as Company-Wide Mark document covers as Company-Wide, using bold font; all other document pages shall also include a Company-Wide Confidentiality header or footer	**Hard copies:** Company employees **Soft copies:** Company employees	Share responsibly and only for business purposes Originators and recipients shall not share the information with persons outside the Company unless those persons have a business need to know	**Hard copies:** Locked cabinet or room **Soft copies:** Minimize the use of removable media	**Hard copies:** No restrictions **Soft copies:** Encrypted - HTTPS, SFTP, FTPS	**Hard copies:** Should be securely disposed of when they are no longer needed – P-2 shredders may be used **Soft copies:** Should be

					storage whenever possible USB Flash, CD-DVD, HDD, Mobile Device. Data Base Server		securely disposed of when they are no longer needed.
3	**Internal use**	Mark as Internal Use Mark document covers as Internal Use, using bold font; all other document pages shall also include a Internal Use Confidentiality header or footer	**Hard copies:** Range of authorized users **Soft copies:** Range of authorized users	In addition to all requirements above: Originators and recipients shall take measures to ensure that access is limited to those with a business need to know Disclosure to non-Company persons or entities shall be subject to a written confidentiality agreement No client or third-party information shall be disclosed unless Company first obtains the written consent of the party that has entrusted such information to Company	**Hard copies:** Locked –Box, Cabinet **Soft copies:** Encrypted USB Flash, CD-DVD, HDD, Mobile Device. Data Base Server	**Hard copies:** Secure packaging Registered mail Signature confirmation **Soft copies:** Encrypted - HTTPS, SFTP, FTPS	**Hard copies:** P-3 Shredded **Soft copies:** Electronic media - wiped, physically destroyed
4	**Confidential**	Mark as Confidential	**Hard copies:** Limited range of authorized users	In addition to all requirements above:	**Hard copies:** Locked –Safe, Metal Box.	**Hard copies:** Secure packaging Registered mail	**Hard copies:** P-4 Shredded

		Mark document covers as Confidential, using bold font; all other document pages shall also include a Confidential header or footer.	**Soft copies:** Limited range of authorized users	Assign dedicated points of contact and create escalation plan in case of a security breach Disciplinary actions may be taken in case a confidential information was disclosed or leaked	**Soft copies:** Encrypted -USB Flash, CD-DVD, HDD, Mobile Device. Encrypted Data Base Server	Signature confirmation Controlled access **Soft copies:** Encrypted - HTTPS, SFTP, FTPS Encryption in transit between Company Information Systems	**Soft copies:** Electronic media - wiped, physically destroyed. Use control measures to witness/record destruction.

Hard copy It is printed on paper. It can't be modified easily. It doesn't need an electronic media for display. It is physical version. It can transmitted physically.	**Soft copy** It is an output copy of document stored in memory and can be seen on screen. It can modified easily. It needs an electronic media for display. It is a digital version. It can be transmitted electrically.

3. General rules

3.1. Disclosure of any information to persons, not being employees of the Company or being employees of the Company but not having access to such information by virtue of a position, is allowed only from the permission of the Head of a Department.

3.2. If an employee, owning information, isn't sure that a particular employee has corresponding authority and access to this information, it is forbidden to disclose this information.

3.3. The employees must follow these rules during all the period of work in the Company and keep it secretly after leaving the Company. Besides, when leaving, an employee shall destroy paper copies of documents belonging to him, and erase information from electronic media.

3.4. The employee shall carry the badge where his photo and name are pointed out for acknowledgement.

3.5. It is forbidden to penetrate and be in premises for the employees who do not have access to these premises.

3.6. An employee, receiving a visitor, shall escort him all time while a visitor is on the Company premises. An employee is responsible for any visitor's action that entails disclosure of information, infringement of work of information systems and etc.

3.7. If an employee has an access to secure premises he/she shall close the door immediately as soon as he/she comes in to or out of secure premises.

3.8. An employee transporting equipment or media, and working with the Company's information out of the office (in a Customer's office, in Internet-cafes, at home, etc.), shall undertake all necessary and reasonable measures to prevent loss and damage of the equipment and unauthorized access to information. In particular, it is not allowed to leave the equipment without supervision (check it as the luggage), type passwords and look through confidential documents if it entails the disclosure of information.

4. Granting information to other employees of the Company and to the third parties

4.1. If the third parties (journalists and others) request an employee to give information or comments, concerning his work at the Company or on Company as a whole, the employee shall inform the Marketing Department or his manager about it.

4.2. If law-enforcement bodies request an employee to provide Company-related information, an employee shall refuse to provide such information, referring to the signed agreement of confidentiality, and promptly inform the Director of Business Support, his manager, the Legal Department Manager or any manager of the Company.

5. Handling of portable computers

5.1. It is strictly prohibited to disable antivirus software and automatic OS updates.

5.2. An employee shall regularly check (not less than once a week) OS latest patches are installed and antivirus bases are up-to-date. If it is discovered it is not, it is shall be updated manually

5.3. The personal firewall shall be enabled if working out of the office.

5.4. An employee shall lock OS (by simultaneous pressing **Win + L**) if leaving the portable computer unattended by whatever reason.

5.5. Unattended portable computer shall be secured with a cable lock (only if required by Customer). The cable lock is provided by Operations Department with portable computer.

5.6. The portable computer shall not be given to any other person for any purpose without any exclusion.

6. Handling of Software, Corporate Equipment and Services

6.1. It is not recommended to open the attachments to e-mails and click URLs received from unknown persons.

6.2. It is forbidden to use corporate email, Internet access, PCs, Laptops and project servers and any other corporate systems and services for private purposes.

6.3. It is forbidden to install or use unlicensed software. Only licensed and freeware software is permitted to install and use on Company equipment. Any software shall be installed and used only within production necessity. It is strictly prohibited to install software used for cryptocurrency mining on PCs, Laptops, project and corporate servers.

6.4. It is strictly prohibited to disable or change settings of anti-virus software and automatic OS updates.

6.5. Change of Operational System settings is allowed only in case of production necessity.

6.6. All Company's employees shall lock their computers (by simultaneous pressing **Win + L**) when leave their workplaces by whatever reason.

6.7. It is forbidden to copy, record, take photos, summarize information and/or communicate it to others to carry out the actions explained above if it is not connected with employee' duties.

7. Remote work

7.1. Technical Prerequisites for remote work

1. Remote access to the corporate network is allowed only through authorized corporate VPN solutions.
2. Remote access to corporate networks and/or corporate applications is allowed only with multifactor authentication.
3. Remote access to corporate networks is allowed only via company-provided equipment (laptops and/or PCs).
4. Corporate equipment must only be used for work-related purposes.
5. Corporate laptops and/or PCs should be enrolled in the company Intune system and managed centrally by the IT department.

7.2. Laptop, PC and Software Handling

1. Keep operating systems and all software up to date.
2. Do not install any software for personal or work purposes that could violate corporate policies and cause claims by third parties, e.g., torrent clients, cryptocurrency miners, etc.
3. Do not disable and/or remove corporate security software on your laptop and/or PC (CrowdStrike, Forcepoint DLP, Antivirus, Zscaler, local Firewall etc.).
4. Do not use unknown or unsecured wireless access points.
5. Use a home router and do not connect your laptop and/or PC to your internet service provider's network directly.
6. Secure your personal wireless network with a strong password.

7.3. Basic rules for mobile work

1. Working documents, data, and information must not be visible nor accessible to unauthorized people.
2. Unauthorized people must not at any time have free access to work IT equipment such as smart phones or laptops.
3. During breaks and when leaving the workplace, PCs and laptops must be locked.
4. After work, it must be secured so that no information is freely accessible
5. Be mindful of physical papers. Keep them in a safe location and bring them back to the office for disposal.

7.4. Rules for working with information in public

1. Work documents and work equipment must not be left unattended or forgotten
2. Data must only be transported on encrypted storage media

3. Consider the security of the environment you intend to work from. Be conscious of who's around you and opportunities for "shoulder surfing" or "eavesdropping", especially when working with sensitive information.

7.5. Transporting equipment

When transporting work equipment, laptops, other mobile devices, and documents, they all must be physically secured against theft. Hence, they must:

1. Only be transported on encrypted storage media
2. Not be left unattended in public areas
3. Not be visible when left in a vehicle for short amount of time (e.g., documents and laptops should be locked in the trunk and covered)
4. Not be left in the vehicle for long periods of time
5. Be carried as hand luggage during flights and railway trips.

8. Choosing a password

8.1. Choosing a password an employee shall take into account the following rules:

- The length of password shall be 14 symbols as a minimum or more;
- The password must include letters in the upper case, letters in the lower case, digits and special symbols in any combination;
- It is forbidden to:
  - Use your name, surname, relatives' names, etc. as a password;
  - Use dictionary words;
  - Write the password anywhere or store it unencrypted way.

8.2. If an employee discovers or even suspects that personal password is disclosed than an employee shall change it immediately and report about all attempts to use personal password by others to IT Department, Information Security Officer and employee's manager.

8.3. All passwords shall be considered to be the information assets of Confidential level.

9. Equipment and Media Treatment

9.1. It is forbidden to open computer's case if it is not authorized by IT Department.

9.2. Carrying-out of equipment and media outside or within the Company is allowed in case of production necessity or with responsible person's approval.

9.3. Originals of all documents shall be stored either electronically or on paper. Electronic representation is preferable.

9.4. The information, the loss of which can affect the ability of the employee or department to carry out his/its duties, shall be stored on server's resources (in departments' folders or employees' private folders, located on network file servers, in version control systems and etc.)

9.5. It is forbidden to store Confidential information on workstations. It shall be stored on server's resources.

9.6. An employee shall restrict the access to his information, stored either electronically or on paper.

9.7. Printouts containing confidential information shall be destroyed by shredder as soon as they are no longer necessary. Care shall be taken to prevent accidental or purposeful access to printed copies for unauthorized persons. A person using the printed copy shall be fully responsible for information safety.

9.8. It is forbidden to leave paper and electronic media containing information of ranks 3, 4 and 5 (according to classification) within view of other persons (on the table, etc.)

9.9. The media and paper containing Confidential Information shall be stored in places with limited access (in safe lockers, fireproof cases, etc.).

9.10. Printed information shall be taken away from printing devices (printers, Xeroxes, faxes and etc.) immediately.

9.11. Any information shall be wiped away off boards and flip-charts after meeting.

9.12. It is forbidden to discuss project or company information loudly.

10. Rules on paper and electronic media utilization

10.1. All paper media containing information of ranks 3, 4 and 5 (according to classification) shall be destroyed by shredder.

10.2. Before delivery the corporate information media (laptops, etc.) to Operational Department or IT Department the containing information of ranks 3, 4 and 5 (according to classification) shall be deleted.

11. Violation of Security Rules

11.1 Intentional or unintentional violation of corporate security policies and rules may lead to penalties up to termination!

12. Reporting security incidents

12.1. Contact the below-mentioned email address with a description of the details of the security incident (e.g., suspicious activities on your work laptop/smart phone, IT systems, theft of confidential information, etc.):

- What happened?
- Who or what is affected?
- How did it happen?
- When did it happen?
- Where did it happen?
- Which information is affected (what is the classification of data: internal, confidential, etc.)?

Email: lux-incident-report@luxoft.com

13. Extraordinary situations

13.1. In case of pressure upon an employee or threat from other persons it is necessary to inform the Head of the Department, Business Support Director or any Company's manager about it.

13.2. If an employee finds out that life-support or access control systems are out of order, they shall inform the reception about it.

13.3. In case of extraordinary situation (such as switching-off electricity, a fire, etc.) it is necessary to act according to instructions of your manager, Business Support Director or any other manager.

List of changes

№	Approval date	Version	Subject of change	Updated/checked by
1	27.02.2017	1.0	Document was reworked to wiki format	I. Zabolotnyaya
2	27.02.2017	1.0	Document was approved	M. Sheraliev
3	06.02.2018	1.1	Document was updated	M. Sheraliev
4	05.03.2019	1.1	Document was reviewed	M. Sheraliev
5	17.07.2019	1.1	Document was updated	M. Sheraliev
6	16.03.2021	1.1	Validity confirmed	N. Nikolaenkova
7	27.12.2021	1.2	"Violation of Security Rules" added	M. Sheraliev
8	14.04.2022	1.3	p. 7. Remote work added, p.12. Reporting security incidents updated	M. Sheraliev
9	21.04.2023	1.4	Scope and Definitions Sections were added Main Steps, p.1 Information classification, p2. Information labeling and handling sections were updated.	A. Maslova