Rules on handling company information

Classification – company-wide

This document presents a set of methods enabling company employees to access the information necessary for them to execute their duties while also preventing third-party or non-approved employee access to information.
The rules describe internal information protection guidelines to be followed by company employees. If information can be considered commercial or official secrets according to relevant legislation and internal company statements (rules on documents containing commercial secrets), the rules for handling this information are determined by applicable legislation and this statute.

The handling and the protection of information are the purview of the CSO.

In this context, "information" is understood to be any official information (categories 2, 3, 4, and 5 according to adduced classification).

Information classification

#	Confidentiality level	Description
1	**Public**	Originates from either within or outside Luxoft and is published for free access (e.g., content of public internet sites or articles in mass media).
2	**Company-wide**	Intended for access and use by all Luxoft employees but not to be disclosed outside of Luxoft (e.g., company-wide rules and regulations or general information on projects).
3	**Internal use**	Restricted information important for department or project performance. Generally accessed and used by all employees of a particular department or project (e.g., department-level regulations or project documentation).
4	**Confidential**	Information important for company performance. Generally accessed by directors and a group of trusted persons (e.g., company plans and materials from management meetings).
5	**Strictly confidential**	Information critical for business. Accessed by a small group of highly trusted persons with additional security measures applied to prevent disclosure (e.g., personal data or salary information).

Information labeling and handling

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

The following regulations apply:

#	Confidentiality level	Labeling	Access management	Data storage	Data transfer	Data deletion and disposal
1	**Public**	**None**	**Hard copies:** No restrictions **Soft copies:** 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**	**None**	**Hard copies:** Range of authorized users **Soft copies:** Range of authorized users	**Hard copies:** No restrictions **Soft copies:** USB flash, CD-DVD, HDD, mobile device, database server	**Hard copies:** No restrictions **Soft copies:** Encrypted - HTTPS, SFTP, FTPS	**Hard copies:** No restrictions **Soft copies:** No restrictions
3	**Internal use**	**None**	**Hard copies:** Range of authorized users **Soft copies:** Range of authorized users	**Hard copies:** Locked – box, cabinet **Soft copies:** USB flash, CD-DVD, HDD, mobile device, database server	**Hard copies:** Locked - box/cabinet **Soft copies:** Encrypted - HTTPS, SFTP, FTPS	**Hard copies:** Shredded **Soft copies:** Electronic media - wiped, physically destroyed
4	**Confidential**	**Required**	**Hard copies:** Limited range of authorized users **Soft copies:** Limited range of authorized users	**Hard copies:** Locked – safe, metal box. **Soft copies:** Encrypted USB flash, CD-DVD, HDD, mobile device. database server	**Hard copies:** Locked – safe, metal box. **Soft copies:** Encrypted - HTTPS, SFTP, FTPS	**Hard copies:** Shredded **Soft copies:** Electronic media - wiped, physically destroyed
5	**Strictly confidential**	**Required**	**Hard copies:** Extremely limited range of authorized users **Soft copies:** Extremely limited range of authorized users	**Hard copies:** Locked - safe **Soft copies:** Encrypted USB flash, CD-DVD, HDD, mobile device. database server	**Hard copies:** Locked in safe and escorted **Soft copies:** Encrypted - HTTPS, SFTP, FTPS	**Hard copies:** Shredded **Soft copies:** Electronic media - wiped, physically destroyed

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

General statements

1. Disclosure of any information to persons who are not company employees or who are entitled to access such information by virtue of their position is allowed only upon gaining permission from the head of the relevant department.
2. If an employee who has access to information isn't sure that a particular employee has the corresponding authority and access to this information, it is forbidden to disclose this information.
3. Employees must follow these rules during their entire the period of work in the company and keep it secret after leaving the company. In addition, when leaving, employees shall destroy paper copies of documents belonging to them and erase information from electronic media.
4. The employee shall carry a badge with their photo and name.
5. It is forbidden for employees who do not have access to restricted premises to be present in these premises.
6. An employee receiving a visitor shall escort them at all times while the visitor is on company premises. The employee is responsible for the visitor's actions that entail the disclosure of information, damage to the operation of information systems, etc.
7. If the employee has access to secure premises, they shall close the door immediately as soon as they arrive or depart the secure premises.
8. Employees transporting equipment or media and working with 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 the loss and damage of the equipment as well as unauthorized access to information. In particular, leaving equipment without supervision (checking it as luggage), typing passwords, and looking through confidential documents are prohibited if they entail the disclosure of information.

Granting information to other company employees and to the third parties

1. If third parties (journalists and others) request an employee provide information or comments concerning their work at the company or on the company as a whole, the employee shall inform the Marketing Department or their manager about it.
2. If law enforcement bodies request an employee provide company-related information, the employee shall refuse to provide such information, referring to the signed confidentiality agreement, and promptly inform the director of business support, their manager, the Legal Department manager, or any company manager.

Handling of portable computers

1. It is strictly prohibited to disable antivirus software and automatic OS updates.
2. Employees shall regularly check (not less than once a week) that the latest OS patches are installed and that antivirus bases are up to date. If they are not, they shall be updated manually
3. Personal firewalls shall be enabled if working out-of-office.
4. Employees shall lock their computer (by simultaneously pressing **Win + L**) if leaving their computer unattended for whatever reason.
5. Unattended portable computers shall be secured with a cable lock (only if required by customer). The cable lock is provided by the Operations Department along with the computer.
6. Company computers shall not be given to any other person for any purpose without exception.

Handling of software, corporate equipment, and services

1. It is not recommended to open e-mail attachments and click URLs received from unknown persons.
2. It is forbidden to use corporate email, internet access, PCs, laptops, project servers, and any other corporate systems and services for private purposes.
3. It is forbidden to install or use unlicensed software. Only licensed and freeware software is permitted for installation 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.
4. It is strictly prohibited to disable or change settings for anti-virus software and automatic OS updates.
5. Changing operating system settings is allowed only in cases of production necessity.
6. All company employees shall lock their computers (by simultaneously pressing **Win + L**) when they leave their workplaces for whatever reason.
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 not connected with employee duties.

Remote work

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.

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.

Basic rules for mobile work

1. It is prohibited to take and work with information that is classified as “Strictly Confidential”. This applies to information both digital and on paper.
2. Working documents, data, and information must not be visible nor accessible to unauthorized people.
3. Unauthorized people must not at any time have free access to work IT equipment such as smart phones or laptops.
4. During breaks and when leaving the workplace, PCs and laptops must be locked.
5. After work, it must be secured so that no information is freely accessible

6. Be mindful of physical papers. Keep them in a safe location and bring them back to the office for disposal.

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.

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.

Choosing a password

1. Employee passwords shall consider the following rules:

    - The length of the password shall be 8 symbols minimum
    - The password must include upper- and lowercase letters, numbers, 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
        - Use the corporate domain account password on any public services. (Facebook, LinkedIn, Gmail, Yahoo, etc.)

2. If an employee discovers or even suspects that their personal password has been disclosed, the employee shall change it immediately and report all attempts to use the password to the IT Department, information security officer, and their manager.
3. All passwords shall be considered strictly confidential information assets.

Equipment and media treatment

1. It is forbidden to open the computer's case if not authorized by the IT Department.
2. Carrying equipment and media outside or within the company is allowed in case of production necessity or with the approval of the person responsible.
3. Originals of all documents shall be stored either electronically or on paper. Electronic representation is preferable.
4. Information, the loss of which can affect the ability of the employee or department to carry out their/its duties, shall be stored on server resources (in department folders or employee private folders located on network file servers, in version control systems, etc.)

5. It is forbidden to store confidential and strictly confidential information on workstations. It shall be stored on server resources.
6. Employees shall restrict access to their information stored either electronically or on paper.
7. Printouts containing confidential and strictly confidential information shall be destroyed by shredding as soon as they are no longer necessary. Care shall be taken to prevent the accidental or purposeful access to printed copies by unauthorized persons. A person using the printed copy shall be fully responsible for information safety.
8. It is forbidden to leave paper and electronic media containing information of levels 3, 4, and 5 (according to the above classification) within view of other persons (on the table, etc.)
9. The media and paper containing confidential and strictly confidential information shall be stored in places with limited access (in safe lockers, fireproof cases, etc.).
10. Printed information shall be taken away from printing devices (printers, Xeroxes, faxes, etc.) immediately.
11. All information shall be wiped off boards and flipcharts after meetings.
12. It is forbidden to loudly discuss project or company information.

Rules on paper and electronic media utilization

1. All paper media containing information of levels 3, 4, and 5 (according to the above classification) shall be destroyed by shredding.
2. Before delivering corporate information media (laptops, etc.) to the Operational Department or IT Department, information of levels 3, 4, and 5 (according to the above classification) shall be deleted.

Violation of security rules

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

Reporting security incidents

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

Extraordinary situations

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 manager about it.
2. If an employee finds out that life-support or access control systems are out of order, they shall inform reception about it.
3. In case of extraordinary situations (such as electrical failure, a fire, etc.) it is necessary to act according to the instructions of your manager, business support director, or any other manager.