**Rules on Company information treatment by employees**

Protection of information, received by employees during their ordinary duty performance – is a set of means of providing Company’s employees 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 Company’s employees. 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.

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, 4 and 5 according to adduced classification).

***Information Classification***

|  |  |  |
| --- | --- | --- |
| **#** | **Confidentiality rank** | **Description** |
| 1 | Public | Origins from either within or outside LUXOFT and 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 is |
|  |  | not to be disclosed outside of LUXOFT (e.g., company-wide |
|  |  | rules and regulations or general information on projects). |
| 3 | Internal use | Information of restricted access, 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 performance of the entire Company. |
|  |  | Generally accessed by Directors and the group of trusted |
|  |  | persons (e.g., Company plans and materials of 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). |

***General statements***

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.
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. 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.
4. The employee shall carry the badge where his photo and name are pointed out for acknowledgement.
5. It is forbidden to penetrate and be in premises for the employees who do not have access to these premises.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ISC-HRM-01 | RULES ON COMPANY INFORMATION TREATMENT BY EMPLOYEES | | | |
|  |  |  |  |  |
| REVISION: 2.1 |  | EFFECTIVE DATE: 30.03.2011 | PAGE: 1 / 4 |  |

1. 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.
2. 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. 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.

***Granting information to other employees of the Company and to the third parties***

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.
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.

***Handling of portable computers***

1. It is strictly prohibited to disable antivirus software and automatic OS updates.
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
3. The personal firewall shall be enabled if working out of the office.
4. An employee shall lock OS (by simultaneous pressing Ctrl+Alt+Del) if leaving the portable computer unattended by whatever reason.
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.
6. The portable computer shall not be given to any other person for any purpose without any exclusion.

***Handling of Software, Corporate Equipment and Services***

1. It is not recommended to open the attachments to e-mails and click URLs received from unknown persons.
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.
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.
4. It is strictly prohibited to disable or change settings of anti-virus software and automatic OS updates.
5. Change of Operational System settings is allowed only in case of production necessity.
6. All Company’s employees shall lock their computers (by simultaneous pressing Ctrl+Alt+Del) when leave their workplaces by 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 it is not connected with employee’ duties.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ISC-HRM-01 | RULES ON COMPANY INFORMATION TREATMENT BY EMPLOYEES | | | |
|  |  |  |  |  |
| REVISION: 2.1 |  | EFFECTIVE DATE: 30.03.2011 | PAGE: 2 / 4 |  |

***Choosing a password***

1. Choosing a password an employee shall take into account the following rules:
   * The length of password shall be 8 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:
   1. Use your name, surname, relatives names, etc. as a password; o Use Russian words in Latin transliteration;

o Write the password anywhere or store it.

1. 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.
2. All passwords shall be considered to be the information assets of Strictly Confidential level.

***Equipment and Media Treatment***

1. It is forbidden to open computer’s case if it is not authorized by IT Department.
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.
3. Originals of all documents shall be stored either electronically or on paper. Electronic representation is preferable.
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.)
5. It is forbidden to store Confidential and Strictly Confidential information on workstations. It shall be stored on server’s resources.
6. An employee shall restrict the access to his information, stored either electronically or on paper.
7. Printouts containing confidential and strictly confidential information shall be destroyed by shredder as soon as they are not 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.
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. 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 and etc.) immediately.
11. Any information shall be wiped away off boards and flip-charts after meeting.
12. It is forbidden to discuss project or company information loudly.

***Rules on paper and electronic media utilization***

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ISC-HRM-01 | RULES ON COMPANY INFORMATION TREATMENT BY EMPLOYEES | | | |
|  |  |  |  |  |
| REVISION: 2.1 |  | EFFECTIVE DATE: 30.03.2011 | PAGE: 3 / 4 |  |

***Incident Reporting***

1. If any violation of security rules covered within this document is discovered or even suspected it shall be immediately reported.
2. The Corporate ServiceDesk system shall be employed to report about security incident choosing the appropriate category.

**Attention!**

It is prohibited to use email or phone to report about security incident except only the case if the ServiceDesk system is inaccessible for an employee. In this case you shall contact ISO or CSO (depends on the DDC) directly and ISO or CSO on behalf of you shall register the Security Incident in ServiceDesk system.

***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’s manager about it.

1. If an employee fined out that life-support or access control systems are out of order, they shall inform the reception about it.
2. 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.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ISC-HRM-01 | RULES ON COMPANY INFORMATION TREATMENT BY EMPLOYEES | | | |
|  |  |  |  |  |
| REVISION: 2.1 |  | EFFECTIVE DATE: 30.03.2011 | PAGE: 4 / 4 |  |