SECURITY POLICIES IN ESSA_2024

This section of the website is dedicated to ESSA's internal policies, which are the basis of how ESSA and its employees manage and operate company and customer data.

The procedures must be completed and are mandatory for all employees.

2.1 Internal security regulation

1. Purpose

The internal security regulation aims to ensure the integrity, confidentiality and availability of information.

The regulation was created so that:

- To be in accordance with the principles expressed by the European Regulation for the Protection of Personal Data (GDPR).
- To establish good practices for the use of the IT and communications system.
- To train the staff of the ESSA Group company regarding the responsibilities associated with accessing and using Personal Data.

The document establishes the rules for the security and control of IT systems, for the fulfillment of confidentiality obligations and the safe keeping of data and information sent or obtained from clients as well as those arising from the activity related to each function.

Headquarter:
Romania, Bucharest, Siret 40 street, Building B, District 1
office@essagroup.ro
+40 21 224 05 20
www.essagroup.ro

2. Scope

The policy is applicable to employees from all S.C ESSA Group SRL departments, in the exercise of the duties, tasks and powers with which they have been vested.

For the purposes of this document, the term "Data" refers to all information, data, knowledge of any kind, acquired, learned, known, in any way and by any means, directly or indirectly, as a result and/or on the occasion and/or in the time and/or in connection with the conclusion, execution, modification and termination of the individual employment contract, the internal regulations, the internal procedures and provisions of the employer, the working schedule, the duties, duties and attributions of the employee, including the personal data of the persons concerned (as defined by the General Data Protection Regulation no. 679/2016), processed by the employer, as operator/associate operator/authorized person.

3. Definitions

The definitions of the terms used are taken from the applicable normative acts.

a) Personal data - any information relating to an identified or identifiable natural person; An identifiable person is that person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, psychological, economic, cultural or

social.

b) Processing of personal data - any operation or set of operations performed on personal data, by automatic or non-automatic means, such as collection, registration, organization, storage, adaptation or modification, extraction, consultation, use , disclosure to third parties by transmission, dissemination or in any other way, joining or combining, blocking, erasure or destruction.

c) Storage - keeping the collected personal data on any kind of support.

Headquarter:
Romania, Bucharest, Siret 40 street, Building B, District 1
office@essagroup.ro
+40 21 224 05 20
www.essagroup.ro

d) Personal data record system - any organized structure of personal data, accessible according to certain criteria, regardless of whether this structure is organized in a centralized or decentralized manner or is distributed according to functional or geographical criteria;.

e) Operator - any natural or legal person, under private or public law, including public authorities, institutions and their territorial structures, which establishes the purpose and means of personal data processing; If the purpose and means of personal data processing are determined by a normative act or on the basis of a normative act, the operator is the natural or legal person, under public or private law, who is designated as the operator by that normative act or based on that normative act.

f) Person authorized by the operator - a natural or legal person, under private or public law, including public authorities, institutions and their territorial structures, who process personal data on behalf of the operator.

g) Third party - any natural or legal person, under private or public law, including public authorities, institutions and their territorial structures, other than the data subject, the operator or authorized person or the persons who, under the direct authority of the operator or authorized person, are authorized to process data.

h) Recipient - any natural or legal person, under private or public law, including public authorities, institutions and their territorial structures, to whom data is disclosed, regardless of whether it is a third party or not; the public authorities to whom data is communicated within a special investigative competence will not be considered recipients.

i) Anonymous data - data that, due to the origin or specific method of processing, cannot be associated with an identified or identifiable person.

j) Security incident – event registered and declared at the entity level regarding the security of information or IT systems with a significant probability of compromising operations and threatening IT security, the consequence of which determined or is likely to determine the compromise of information or computer systems.

k) Vulnerabilities - states of fact, processes and/or phenomena that reduce the ability of IT systems to react to existing or potential risks or that favor their appearance and development, with consequences in terms of functionality and utility.

4. General security rules

It is the responsibility of each employee of the company to adhere to these Rules and Procedures, to know and apply the present provisions.

Headquarter:
Romania, Bucharest, Siret 40 street, Building B, District 1
office@essagroup.ro
+40 21 224 05 20
www.essagroup.ro

Users, through their actions, must not attempt to compromise the protection of information and communication systems and must not carry out, deliberately or accidentally, actions that may affect the confidentiality, integrity and availability of data of any type within the ESSA Group's IT system.

Employees must not allow family members or other unauthorized foreign persons, who do not have explicit approval from the company's management, access to the company's IT system.

Users must not use USB sticks, external hard drives, or any other magnetic medium for storing information from outside the company without the explicit consent of management.

Users must not download, install and run security programs or utilities that expose or exploit security vulnerabilities of the company's IT and communications system.

No user of the computer system can disclose the information to which he has access or to which he had access as a result of a vulnerability of the computer system. This rule also extends after the user has terminated relations with the company, according to personal commitments or signed employment contracts, existing within the Human Resources Service.

All employees have the obligation to participate in the Data Security training organized by the company.

5. Physical Access

Each employee is responsible for the workstation and implicitly for the related office.

Access to the buildings and office spaces of the company is made only on the basis of an access card. The access card cannot be transferred for any reason.

The personnel who have access rights must have a service card and identity documents attesting to their status.

The access of foreigners to the office spaces will be done only on the basis of the identity document. Visitors/foreign persons must be accompanied in the company's office premises.

Each employee is responsible for immediately notifying the security staff of the presence of an unaccompanied foreign person who is not authorized to access the office premises.

Employees who work in areas exposed to visitors or with monitors facing outside windows must use a monitor filter system to reduce the visibility of outside data.

When leaving the office, the employee has the responsibility to lock the workstation. (Windows Lock)

Headquarter:
Romania, Bucharest, Siret 40 street, Building B, District 1
office@essagroup.ro
+40 21 224 05 20
www.essagroup.ro

The employee is responsible for the security of all devices on which data is stored or through which data can be accessed (laptops, phones, tablets, memory cards, USB sticks, external hard drives, etc.). In this sense, he must ensure that they are not left unattended in the common spaces of the company's buildings or in public spaces.

All employees are responsible for maintaining all documents in physical format in files/libraries/files. It is not allowed to keep any document containing data on the desk, in plain sight.

If there are documents to be picked up by visitors, they will not be stored on the desk in plain sight, but in secure files.

Physical documents that are no longer needed in the employee's activities will be sent for archiving or destruction, according to the indications of internal procedures.

6. Accessing the computer system

Access to the computer system can only be done through authorized workstations.

It is the employee's responsibility to ensure that the devices used to access the computer system (laptop, mobile phone, tablet) comply with the device security requirements described in the internal procedure. These include but are not limited to:

- Supported operating system versions – Windows 7, Windows 8, Windows 10.
- The existence of an operating system access password
- Using an authentication method to unlock the mobile phone (PIN, Password, Fingerprint, etc.)
- The complexity of the access password and the validity period
- Activation of the automatic user disconnection function after a period of inactivity.
- Deactivation of "Guest" accounts
- Encryption of the local partition intended for company activities
- Activation of the Firewall function of the operating system
- Installing and activating an anti-virus software
-

- Installation of any program required by the company management or mentioned in the internal procedure;
- Starting the automatic installation function of the packages intended for the operating system;
- Each employee has a unique account through which his authentication and authorization is carried out in the IT system.
- Employees must not disclose or alienate account names, passwords, Personal Identification Numbers (PINs), authentication devices or any similar devices and/or information used for authorization and identification purposes.

7. Confidentiality and Data Integrity

The use of the computer system or the access and use of the Data in digital or physical form by unauthorized persons is prohibited.

Employees must not attempt to gain access to Data for which they do not have express authorization or consent.

To obtain an access authorization, employees can send a request in which they mention the resources they want to access and the reason, to the email address: acces@essa.ro.

Employees must not make unauthorized copies of the Data.

8. Data storage and transfer

It is allowed to store Data only in the following ways:

In the online sites (Microsoft SharePoint) designated by the company's management and authorized according to internal procedures.

On workstations, in partitions created especially for ESSA activities, encrypted according to internal procedures.

In exceptional situations, the Data can be stored on authorized external storage media (USB sticks, external hard drives) only if they have been encrypted in advance according to the internal procedure.

Headquarter:
Romania, Bucharest, Siret 40 street, Building B, District 1
office@essagroup.ro
+40 21 224 05 20
www.essagroup.ro

It is strictly forbidden to store Data in digital format using applications, storage media or other unauthorized devices.

The transfer of files containing Data to other employees of the company or to clients or authorized third parties is done only through the online site (Microsoft Sharepoint) designated by the company's management, according to the internal procedure.

If it is necessary to send photos using a mobile phone, this is only allowed through the Microsoft SharePoint/OneDrive mobile application. It is necessary to delete the photos from the mobile phone after uploading them successfully.

After successfully uploading the working documents in the Sharepoint space, the copies of the documents must be deleted from the workstation and from the external storage media.

9. Security Incidents

Users are obliged to report any anomalies in the performance of the systems used as well as any signs of possible crimes by sending an email to the email address security@essa.ro.

In case of loss or theft of computing devices (laptops, phones, tablets), employees are obliged to report the incident using the email address security@essa.ro.

2.2 Physical security

The security policy establishes the management infrastructure for the identification and management of security threats.

Physical security is divided into:

1. Pick up visitors

- Reception of visitors from the entrance to the company by a person specially delegated for this purpose.
- Drafting of a regulation regarding the regime of visitors.
- Introduction of visitor badges.

Headquarter:
Romania, Bucharest, Siret 40 street, Building B, District 1
office@essagroup.ro
+40 21 224 05 20
www.essagroup.ro

- Visitors will be accompanied by the designated person throughout their stay in the company.
- Small instruction for visitors regarding the company's security policy (they cannot use the company's work equipment, they are not allowed to take photos inside the company, etc.).

2. Video security

- The company must take the necessary steps to install a surveillance system suitable for the headquarters where it operates.
- Surveillance cameras will be installed in the work spaces as well as in the physical archive.
- Access to the records related to this system should be limited to the general director/IT manager level.
- Access to the company should be based on cards (magnetic, RFID)
- Installation of motion sensors and alarm system in case of burglary.
- Creating restricted access areas.

3. Job security

Each employee must be responsible for the workstation and implicitly for the related office.

Every time he leaves the office, he must lock the workstation by means of Windows lock.

Those who work in areas exposed to visitors or with monitors facing the outside windows should use a monitor filter system to reduce the visibility of outside data.

All documents in physical format are files/libraries/files, the office must be permanently empty.

If there are documents to be picked up by visitors, they will not be stored on the desk in plain sight, but in secure files.

People who work with physical documents must have secure files and shredders for destroying expired documents that contain personal data.

4. Securing archives

The archives in physical format will be stored in an appropriate space according to legislative requirements.

A position of archiving manager will be established.

Headquarter:
Romania, Bucharest, Siret 40 street, Building B, District 1
office@essagroup.ro
+40 21 224 05 20
www.essagroup.ro

The archiving manager ensures that the documents are stored, inventoried and identifiable accordingly.

A commission for the destruction of documents that have exceeded the retention period will be drawn up, and the person in charge of archiving must also be part of it.

An archive register will be drawn up where the archive manager will note which documents leave the archive, to whom they go and when they return.

2.3 Security of ESSA Applications and Platforms

All applications developed for ESSA campaigns must comply with the following security requirements:

1. Access to platforms / applications

a) Access to the developed applications and platforms must be done through accounts and unique authentication passwords for each person.

b) For each new application, users are created based on a list received from ESSA at the beginning of the campaigns/projects.

Each user will receive access information through a secure method (encrypted email or other methods approved by ESSA). This information will be sent individually for each user.

Every user must be obliged to change his password at the first login.

The set password must comply with the following security requirements:

Complex password: which should include lowercase letters, uppercase letters, numbers and special characters.

The minimum length of the password should be 6 characters.

Password to expire every 90 days (for situations where applications are used for more than 90 days).

Headquarter:
Romania, Bucharest, Siret 40 street, Building B, District 1
office@essagroup.ro
+40 21 224 05 20
www.essagroup.ro

When new or reset passwords are set, the re-use of old passwords must not be allowed up to the last 12 passwords.

c) Any access request received after the start of a project must be approved by the DPO designated within ESSA.

Developers have the obligation to send these requests to the DPO at the address provided by ESSA and wait for confirmation.

2. Actions allowed within the platforms / applications

Every application / platform developed must allow the restriction of the activities performed on the data (eg listing data, modifying data, deleting data, etc.).

Each user must receive limited access to the data within the application.

The access level is set at the beginning of the campaigns/projects through a list of access requirements received from ESSA.

Any request to configure an additional access for any user must be approved by the DPO designated within ESSA.

Developers have the obligation to send these requests to the DPO at the address provided by ESSA and wait for confirmation.

Disclosure of root/administrator/super-user accounts to ESSA employees is prohibited.

3. Auditing activities

All the activities that take place on the developed platforms/applications must be recorded in an activity log (eg: authentication, password reset, data listing, data editing, data deletion, etc.).

These logs must be distributed to ESSA at their request and at the end of each campaign / project.

All reports created by ESSA users or by developers (at the request of ESSA employees) must be recorded in a data processing log. This log must be distributed to ESSA at their request and at the end of each campaign / project.

4. Interaction with the platforms

Headquarter:
Romania, Bucharest, Siret 40 street, Building B, District 1
office@essagroup.ro
+40 21 224 05 20
www.essagroup.ro

Each platform / application must automatically disconnect the user after a period of inactivity of 30 minutes.

The Platforms / Applications must allow the identification and deletion of a specific entry of a target person (registered consumer) upon ESSA's request.

5. Security of servers

The servers on which the platforms are developed must be secured with firewall, anti-virus and malware protection systems.

Connection interfaces (ports) between client devices and servers must be limited to the minimum necessary.

Communications between client devices and servers must be encrypted with TLS or other similar technologies.

Communication with the servers used must be limited to the client devices that will connect and the administration of the platforms.

If there are several servers, the networks to which they are connected must be secured and limited regarding access from the outside.

The servers used by the developed platforms/applications must be encrypted at the storage level, using AES or similar technologies.

The keys used for encryption must be secured and changed regularly.

If the servers are replaced, the data on the old servers must be irreversibly destroyed.

The servers and databases used must be redundant from the perspective of storage media, physical servers (High Availability)

There must be duplication of hardware, software and infrastructure systems (eg by replicating hard drives, power supply).

There must be backup procedures for the servers and databases used.

The backups made at the database level must be independent for each application / platform developed and must be deleted at the end of a campaign / project.

The servers must be kept in data center facilities with all related functionalities, such as:

- Conditioning system
- Dust filtration system

Headquarter:
Romania, Bucharest, Siret 40 street, Building B, District 1
office@essagroup.ro
+40 21 224 05 20
www.essagroup.ro

- Secure server rooms
- Emergency plans
- Disaster recovery
- Ensuring sufficient capacity of IT systems and facilities
- Firewall, IDS network protection
- Data resilience and error management
- Implementation of repair strategies and alternative processes
- Emergency Tests / Activity Recovery Tests
- Penetration tests
- Connecting to these servers by developers must be done using secure workstations with firewall, anti-virus and up-to-date patched systems.

6. Interaction with saved data

The developed platforms/applications must ensure the operational capacity to compile, correct, block and uniformly delete all personal data stored about a person.

The platforms must allow the export of all data collected at the request of ESSA as well as at the end of each campaign / project.

This export must be limited to normal users.

This export must be done only by the application developers.

The export must be transmitted securely to ESSA.

ESSA will provide you with a SharePoint location for each application / project.

This location and the upload of the export is secured through https connections.

The existence of an https connection must be confirmed by the developers before uploading the data.

Exporting by any other method (USB stick, emails, ftp connections) is NOT allowed.

At ESSA's request, the data specific to a campaign/project must be completely deleted.

The deletion must be confirmed by email to ESSA.

Headquarter:
Romania, Bucharest, Siret 40 street, Building B, District 1
office@essagroup.ro
+40 21 224 05 20
www.essagroup.ro

The deletion must be done in an irreversible way, by using modern methods/techniques (eg overwriting the storage area used by the application).

7. Application development methods

All applications / platforms developed must comply with security concepts according to:

- OWASP Secure Web Application Framework Manifesto: https://www.owasp.org/index.php/OWASP_Secure_Web_Application_Framework_Manifesto
- OWASP Mobile Security Project: https://www.owasp.org/index.php/OWASP_Mobile_Security_Project

It is the responsibility of the developers to follow all current cyber attacks / vulnerabilities / back doors that could affect the applications, platforms, servers, databases used in the development of ESSA applications / platforms and to apply the necessary measures to prevent these attacks /vulnerabilities.

Developers must respond to any request for information regarding attacks and vulnerabilities from ESSA with details about the protection measures applied. This answer must come within 3 days of receiving the questions from ESSA.

Developers must respond within 3 days to all technical questions from ESSA or the representatives chosen by ESSA during the audit processes that can take place every 3 months, annually or at any time.

For each new application developed for an existing / new client, at the request of ESSA (according to the DPIA process - Data Privacy Impact Assessment), the developers must provide the technical documentation of the application in which the operation of the application, all the components and the implemented security measures are described.

Data stored directly on client devices (tablets, phones, etc.) must be encrypted and inaccessible by the users of these applications by other methods than using the application developed for the campaign / project.

Developers must ensure an isolated testing environment during the period in which the applications / platforms are created. Separated from the production environment in which the applications will run during the campaigns / projects.

Headquarter:
Romania, Bucharest, Siret 40 street, Building B, District 1
office@essagroup.ro
+40 21 224 05 20
www.essagroup.ro

The applications that will collect personal data must include options to approve the collection by the consumer. This opt-in must be clearly presented by the application (tick, check-box, etc.) and be saved in the databases where these data are stored.

The applications must also contain notification messages regarding the protection of personal data made available by ESSA.

Document management

Name of the document	Security policies in ESSA
Owner	Juridic department, Cyber Security dept.
Applied to:	ESSA GROUP – management, implementation, clients, suppliers
Date of writing	**January 2019**
Approved by:	Eugen Saulea, CEO
Contact for questions	security@essagroup.ro
Last update	**January 2024**