DATA SECURITY POLICY

Creation and modifications						
Version	Written by	Reviewed by	Approved by	Description	Activities	Confidentiality
V1	Guy Sadoun DPO 01/09/2020	NA	Cédric Castro CEO 22/09/2020	Creation	ALL	Internal
V2	Guy Sadoun DPO 15/03/2021	NA	Cédric Castro CEO 22/03/2021	Update	ALL	External
V3	Raphael Richer IT Director 08/12/2023	Guy Sadoun DPO 12/12/2023	Cédric Castro CEO 15/12/2023	Update	ALL	External
V4	Raphael Richer IT Director 24/06/2024	Guy Sadoun DPO 10/07/2024	Cédric Castro CEO 10/07/2024	Update	ALL	External
V5	Raphael Richer IT Director 30/10/2025	Guy Sadoun DPO 31/10/2025	Cédric Castro CEO 19/11/2025	GDPR Reference	ALL	External

Table des matières

1. Introduction

The Data Security Policy (DSP) provides information on the prescribed measures used to establish and enforce the Information Security Program in the Mobilitas Group (MOBILITAS). (in accordance with Article 32 of the GDPR).

MOBILITAS is committed to protecting its employees, partners, customers, and agents from damaging acts, whether intentional or unintentional. Security is a team effort involving the participation and support of everyone who interacts with data and information systems. Therefore, it is the responsibility of every user to know these policies and to conduct their activities in accordance with these policies.

Protecting MOBILITAS, client, partner, and agent information and systems that collect, process, and store this information is critical. The security of data and information systems must include controls and safeguards to offset possible threats and reduce exposure to risk as well as ensure the confidentiality, integrity, and availability of data. Security measures must be taken to guard against unauthorized access to, alteration, disclosure or destruction of data and information systems; this includes accidental loss or destruction, (in accordance with the principles of Articles 5, 6 and 25 of the GDPR).

2. Purpose

The purpose of the DSP is to prescribe a comprehensive framework for:

- Protecting the confidentiality, integrity, and availability of MOBILITAS data and information systems, (in accordance with the principles of Articles 5, 6 and 25 of the GDPR).
- Protecting MOBILITAS, its employees, clients, and agents from illicit use of MOBILITAS information systems and data
- Ensuring the effectiveness of security controls over data and information systems that support MOBILITAS's business operations, (in accordance with the principles of Articles 5, 6 and 25 of the GDPR).
- The evolution of minimum-security controls required to protect MOBILITAS's data, information systems, and business operations, (in accordance with the principles of Articles 5, 6 and 25 of the GDPR).

3. Scope and Applicability

These policies, standards, and procedures apply to all MOBILITAS data, information systems, activities, and assets owned, leased, controlled, or used by MOBILITAS, its agents, contractors, or other business partners on behalf of MOBILITAS. These policies, standards, and procedures apply to all MOBILITAS employees, contractors, sub-contractors, and their respective facilities supporting MOBILITAS business operations, wherever MOBILITAS data is stored or processed, including any third party contracted by MOBILITAS to handle, process, transmit, store, or dispose of MOBILITAS data, (in accordance with the principles of Articles 5, 6 and 25 of the GDPR).

All personnel supporting or processing MOBILITAS business functions shall comply with the DSP. MOBILITAS business units, partners, or agents may create and use a more restrictive policy, but not one that is less restrictive, less comprehensive, or less compliant than this policy. This policy does not supersede any other applicable law, existing labor management agreement, or government regulation in effect as of the effective date of this policy, (in accordance with the principles of Articles 5, 6 and 25 of the GDPR).

4. Violations

MOBILITAS employees have signed an IT charter, a text drawn up by the company to define the rules for the use of information systems, which applies to any person authorized to access and use them in the exercise of their professional activities, regardless of their status, employee, temporary worker, trainee, employee of service providers, etc. It is imposed unilaterally by MOBILITAS to make each user aware of the issues in terms of security and privacy protection. (in accordance with the principles of Articles 5, 6 and 25 of the GDPR).

Personnel supporting or processing MOBILITAS business that are found to have violated the DSP will be subject to disciplinary action, up to and including termination of employment and/or termination of association with MOBILITAS. Violators of local, state, Federal, and/or international law will be reported to the appropriate law enforcement agency for civil and/or criminal prosecution, (in accordance with the principles of Articles 5, 6 and 25 of the GDPR).

5. Information Security Program (in accordance with Article 32 of the GDPR)

MOBILITAS shall protect the confidentiality, integrity, and availability of its data and information systems. Security controls will be tailored accordingly so that cost-effective controls can be applied based on the risk and sensitivity of the data and information, in accordance with all legal obligations, (in accordance with the principles of Articles 5, 6 and 25 of the GDPR).

a. Management Commitment to Information Security, (in accordance with Article 32 of the GDPR)

MOBILITAS management is committed to the protection of information assets. Management demonstrates its commitment to information security through its adherence to the following fundamental principles: (in accordance with Article 32 of the GDPR)

- Treating information as a critical business asset.
- Incorporating high standards of corporate governance to all data elements stored, processed and transmitted.
- Demonstrating to customers and business partners that the enterprise deals with information security in a professional manner, (in accordance with the principles of Articles 5, 6 and 25 of the GDPR).

- Ensuring that the enterprise has a set of security policies that implement controls over information and systems that addresses confidentiality, integrity, and availability, (in accordance with Article 32 of the GDPR).
- Management further demonstrates its commitment to information security by engaging in the following actions, (in accordance with Article 32 of the GDPR) :
    - Assigning overall responsibility for information security to a member of senior management.
    - Allocating dedicated organizational resources to information security.
    - External review (third party) of the IS policies to ensure they are meeting or exceeding industry best practices.

b. Organization of Information Security (in accordance with Article 32 of the GDPR)

The authority and responsibility for managing the information security program are delegated to MOBILITAS's Information Security Officer (ISO) who has responsibility for, (in accordance with Article 32 of the GDPR):

- Establishing, documenting, and distributing information security policies, procedures, and guidelines.
- Defining, implementing, and supporting a set of security services which provide a range of security capabilities.
- Providing expert advice on all aspects of information security.
- Overseeing the investigation of information security incidents.
- Escalate security alerts to appropriate personnel.
- Contributing to information security awareness programs and developing security skills for staff.
- Evaluating the security risks and implications of business initiatives and procurement of services, (in accordance with the principles of Articles 5, 6 and 25 of the GDPR).
- Working cooperatively with internal and external auditors in the auditing of security practices.
- Partnering with internal groups that have related responsibilities (i.e., Law, Treasury/Audit, Human Resources), (in accordance with the principles of Articles 5, 6 and 25 of the GDPR).
- Monitoring and analyzing security alerts and information.
- Reviewing standards for applicability
- Revising standards to address organization changes

c. General Awareness and Training of Information Security (in accordance with Article 32 of the GDPR)

Specific activities are undertaken to promote security awareness to all associates who have access to information and systems that are supporting MOBILITAS business. These activities are:

- Endorsed and promoted by management.
- Delivered as part of associate new-hire orientations and as part of on-going associate training, to occur at minimum annually.
- Aimed at providing associates with specific expectations of their role in securing, protecting, and handling information.

- Aimed at reducing the frequency and magnitude of information security incidents, (in accordance with Article 32 of the GDPR)
- Role-based security related training will occur before authorizing access to data or systems required for assigned job duties.

d. Identification of Information Security Controls (in accordance with Article 32 of the GDPR)

MOBILITAS uses the following sources for the identification of security requirements:

- Risk assessments
- Internal and external penetration tests
- Internal and external vulnerability assessments
- Statutory, regulatory, and contractual requirements that MOBILITAS must satisfy.
- Principles, objectives, and business requirements for information handling that MOBILITAS has developed to support its operations.

e. Assessments

The results of risk assessments, vulnerability assessments, and penetration tests assist in identifying threats to assets, vulnerabilities and the likelihood of occurrence, and potential estimated business impact. These assist in determining appropriate management action, priorities for managing risks, and implementation of protection measures. The following represents MOBILITAS's approach to information security risk assessment, (in accordance with Article 32 of the GDPR):

- The scope of assessments can be either the whole organization, parts of the organization, a specific information system, or a specific component of an information system.
- Assessments will have a clearly defined scope to be effective and will include relationships with risk assessments from other areas as appropriate (i.e., Law, Human Resources, Finance, etc.).
- Assessments may be performed internally, by a third-party, or a combination of both.
- Expenditures on controls to address risk will be balanced against the business harm likely to result from security failures, (in accordance with the principles of Articles 5, 6 and 25 of the GDPR).
- Before considering the control of a risk, criteria will be established for determining whether the risk can be accepted. Risks may be accepted if, for example, it is assessed that the risk is low or that the control is not cost-effective for the organization. Such decisions should be recorded.
- Assessments shall be conducted, at minimum, annually.

f. Data Classification and Handling

Determining how to protect and handle data and information depends on the type of information, importance, and usage. Classification is necessary to understand which security practices and controls should be applied to the data in order to provide the appropriate level of protection. The more sensitive the data, the tighter the controls need to be on that data. All data is classified as Confidential, Manager, Internal, Supplier and External as defined in Appendix 1.

Data should be handled according to its classification. Specialized data handling procedures may be required for Manager and Confidential data; in addition, specific customer data may have additional handling instructions that MOBILITAS has agreed to contractually. Prior to handling or processing data,

users should ensure they understand the proper and/or required handling procedures and are following them appropriately.

g. Legal, Regulatory, and Contractual Compliance

MOBILITAS will ensure compliance with relevant statutory, regulatory, and contractual requirements affecting information security. The information security organization will work collaboratively with other MOBILITAS entities, including Legal, Risk Management, Human Resources, and Contracts to evaluate the applicability of MOBILITAS information security controls to new and existing legislation or regulatory requirements, (in accordance with Article 32 of the GDPR).

6. Access Control

Access controls are designed to reduce the risk of unauthorized access to MOBILITAS data and to preserve and protect the confidentiality, integrity, and availability of MOBILITAS systems. All assigned access shall be reviewed and audited for accuracy to ensure employees only have access to the data required for them to perform their assigned operational duties. Access reviews shall occur, at a minimum, every 6 months, (in accordance with the principles of Articles 5, 6 and 25 of the GDPR).

a. User Access Management

The Security Administration team is responsible for ensuring proper user identification and authentication management by enforcing a formal, documented, provisioning and de-provisioning procedure as follows:

- Centralized control regarding addition, deletion, and modification of user accounts and credentials to ensure authorized use is maintained.
- Immediately revoke access for any terminated user, (in accordance with the principles of Articles 5, 6 and 25 of the GDPR).
- Disable or remove inactive accounts at least every 90 days.
- Limit repeated access attempts by locking out an account after no more than five failed attempts.
- Require an administrator to unlock any disabled account.
- Track and monitor role assignments for privileged user accounts.
- Enable accounts used by vendors for remote access only during the period they are needed.
- Ensure assigned access provides adequate separation of duties for all employees

b. Least Privilege

The principle of “least privilege” access, which states only the minimum level of access will be granted to perform the assigned operational duties, shall be used when granting employees access to systems or data. Access shall not be granted without an approved business requirement and management approval.

c. Identification and Authorization

Each individual employee is provided with a unique user identity for the purpose of identification, authorization, and authentication to systems processing MOBILITAS data or supporting MOBILITAS business functions. This unique identity, associated credentials, and password is considered confidential information and should only be used by the individual it is assigned to. Sharing of unique user identities,

associated credentials, or password is not permitted. In the event of a locked account, individuals are only permitted to request their unique account to be unlocked and the individual's identity will be verified prior to the account being unlocked, (in accordance with the principles of Articles 5, 6 and 25 of the GDPR).

d. Password Management

Passwords are considered confidential and therefore should not be written down or stored in an unencrypted format. Passwords, password complexity, and password lifecycle should adhere to Mobilitas Password policy. Forbidden actions related to passwords include, but not limited to, the following:

- Do not use default vendor passwords
- Do not reveal a password over the phone to anyone
- Do not send your password to anyone via email
- Do not share or tell your password to others
- Do not write your password down

7. Operational Security

Operational security processes are used to identify critical data and systems, the vulnerabilities associated with them, and to determine the appropriate risk mitigations that are needed to ensure MOBILITAS operations are not negatively impacted.

a. System Hardening

System hardening procedures should be defined and followed for all systems and platforms (workstations, servers, databases, etc.), both production and development, to reduce the risk of systems being compromised. These procedures should be consistent with industry-accepted hardening standards and include, but not limited to:

- Procedures and standards updated as new vulnerabilities are identified
- Applied when new systems are configured, prior to being connected to the production network
- Follow the 'least privilege' access model
- Remove unnecessary functionality
- Implementing security features as relevant (SSH, TLS, etc.)
- Removal of all default vendor accounts and passwords
- Installation of anti-virus software
- Installation of Endpoint management application
- Appropriate level of monitoring and logging is enabled and retained to allow review after a service impacting event is encountered

In addition to the above hardening standards, the following steps shall be taken to further protect systems and reduce risk:

- Establishing owners of each system and assigning responsibility to personnel that are technically capable

- Ensuring that privileged access to systems is restricted to authorized personnel only
- Following defined access management procedures when generating system access
- Designing systems to operate with current and predicted load levels
- Separating production and testing systems
- Limiting the use of production data in test environments
- Monitoring and supervising the activities of personnel responsible for systems
- Ensuring the appropriate level of replication and/or backups are configured
- Using industry accepted levels of encryption for data at rest, transit, and processing when technically feasible
- Identifying end of life components and planning appropriately for migrations to supported versions prior to end of support/life
- Ensuring the appropriate level of redundancy is configured and available to reduce single points of failure
- The installation of software on systems is restricted to authorized personnel only
- Processing and storage capacity planning is conducted appropriately to ensure business growth needs are met
- Appropriate use of firewalls, intrusion detection, and intrusion prevention, and log aggregation systems

b. Patch Management

Routine installation of vendor-issued updates and patches (operating system, security, etc.) are necessary to protect systems and data from compromission. All systems (workstations, servers, network devices, firewalls, routers, mobile devices, etc.) should routinely and regularly be patched. At a minimum, general patches should be installed quarterly while critical security patches should be applied as soon as possible. Proper testing of patches in a test environment, prior to release on production systems, is crucial to ensure interruptions to operations is not encountered.

c. Change Management

Change control processes are followed to maintain the integrity of production and non-production systems, to ensure that standardized methods are used for handling of all changes, and to minimise the impact of change related incidents. The Mobilitas ISMS Change Management policy must be followed to ensure the following steps are done properly:

- Clear definition of the change requested
- Review of the request
- Impact analysis
- Approval of the change
- Prioritization and planning of implementation
- Documenting all aspects of the change

d. Asset Management

MOBILITAS personnel, business partners, agents, and contractors shall protect assets associated with MOBILITAS operations by ensuring appropriate handling requirements are followed to prevent unauthorized disclosures regardless of if assets or data are being stored or transmitted. All assets

associated with data or with data processing shall be inventoried and tracked. The inventory shall include, but not limited to, (in accordance with the principles of Articles 5, 6 and 25 of the GDPR).

- A list of all devices
- Method to accurately and quickly determine the owner
- Contain contact formation for the asset owner
- Be updated promptly as necessary

e. Physical Security

A defined and documented physical security program and procedures shall be used to ensure the physical protection of all systems associated with MOBILITAS business. The physical security program shall include, but not limited to:

- Security perimeters should be defined and used to protect areas that contain MOBILITAS data or systems
- A list of personnel with authorized access to the facility and promptly remove access as necessary
- Use of access control mechanisms (access badge, biometrics, etc.) where possible
- Issue authorization for physical access
- Strictly limit access to sensitive areas and/or areas that contain systems processing MOBILITAS data
- Use video surveillance and other recording and/or logging devices when possible
- Register and log all visitor access to the facility
- External visitors must be always accompanied

8. Disaster Recovery and Business Continuity

Disaster Recovery (DR) and Business Continuity (BC) refer to responding to operational interruption through the implementation of a recovery plan. The recovery plan accounts for applications deemed critical for business operations, service delivery, and ensures the timely restoration of MOBILITAS's capability to deliver services. The DR/BC plan should be tested, at minimum, annually to ensure the plan is up to date and capable of sustaining business operations during a period of disruption, (in accordance with the principles of Articles 5, 6 and 25 of the GDPR).

MOBILITAS, and those conducting MOBILITAS business shall:

- Develop a contingency plan for business-critical systems that:
  - Provides recovery objectives and restoration priorities
  - Determines contingency roles, responsibilities, and assigned individuals
  - Addresses maintaining essential business functions during a disruption
  - Addresses full system restoration
  - Is reviewed and approved by designated company senior personnel
- Communicate contingency plan throughout the organization and ensure assignments are understood
- Coordinate contingency planning and plan reviews at least annually
- Modify the plan accordingly to address business changes
- Establish procedures to access data and systems during periods of disruption

- Ensure defined plans and procedures meet and adhere to contractually obligated recovery timelines and/or objectives

9. Incident Management (in accordance with Article 33 of the GDPR)

Incident management refers to the actions taken to address an event that either creates service disruption or impacts a customer. The criticality of an incident can vary based on its impact on the organization. Incident response procedures should be periodically reviewed to ensure the defined steps are current and applicable to the existing environment. To have an effective response to an incident, there must be a defined, repeatable process that is followed. As indicated in the group Incident Management policy, MOBILITAS addresses incident response by applying these main steps to all encountered incidents, (in accordance with Article 33 of the GDPR):

- **Declaration of the incident**: incident is reported to the Incident Response Team
- **Identification and classification**: Identify impacted assets and the criticality of the incident
- **Incident response actions:**
  - Assessing the incident: Determining the scope, impact, and root cause of the incident.
  - Containment: Taking immediate steps to prevent further damage or loss by isolating affected systems, disabling compromised accounts, or blocking access points.
  - Eradication: Removing the cause of the incident, such as removing malware, patching vulnerabilities, or fixing misconfigurations.
  - Recovery: Restoring affected systems, data, and services to normal operation.
  - Investigation: Conducting a thorough analysis of the incident to understand the full extent of the breach, identify lessons learned, and take appropriate preventive measures.
  - Documentation: Documenting all relevant incident details, actions taken, and recommendations for future improvements. This will be done using the group “Incident Report Template”.
  - Communication: communicate to impacted parties (internal users, clients, vendors,…) and relevant authorities.

10. Software Development Life Cycle

A Software Development Life Cycle (SDLC) is a series of steps that provides a framework for developing and managing software throughout its life cycle. When implemented correctly, a SDLC ensures that that highest quality software is delivered in a quick time, for the lowest overall cost. All development activities at MOBILITAS follow a defined SDLC which takes into account the following items:

- Training
- Define security and design requirements
- Define compliance metrics and reports
- Perform threat modeling
- Define and use cryptographic standards
- Manage the security risk of using third-party components
- Use approved tools
- Perform static analysis security testing (SAST)

- Perform Dynamic Analysis Security Testing (DAST)
- Perform penetration tests
- Establish a standard incident response process

During this process, attention is given to clearly identify the functionality requirements, remedy the code of vulnerabilities and bugs, ensure it meets the stakeholder's needs, and is safe to deploy into the production environment. The SDLC is followed for all feature enhancements, upgrades, etc. until the product is discontinued and removed from service.

11. Acceptable Use

Employees are granted access to MOBILITAS equipment and systems to assist them in performing their job. The equipment and systems belong to MOBILITAS and use is intended only for legitimate, business purposes. Without prior notice, MOBILITAS may review any material created, stored, sent or received on its systems or equipment. All employees using MOBILITAS systems or equipment are obligated to use these items responsibly, professionally, ethically, and lawfully, (in accordance with the principles of Articles 5, 6 and 25 of the GDPR).

a. Equipment and System Usage

Users shall:

- Immediately report: all lost or stolen equipment, known or suspected privacy or security incidents
- Log off or lock systems when leaving them unattended
- Complete all required security and privacy training
- Follow appropriate data handling procedures
- Be vigilant when access the internet and verify all material safe before viewing
- Follow the "Clean Screen, Clean Desk" mentality to protect data,
- Follow all defined record retention policies
- Only connect to known and trusted networks
- Speak only for yourself on social media accounts as you could mistakenly be viewed as a spokesperson for MOBILITAS in your online communications, (in accordance with the principles of Articles 5, 6 and 25 of the GDPR).
- Only use MOBILITAS systems and equipment for their intended business purpose
- Adhere to MOBILITAS's privacy policy, code of conduct, and data security policy, (in accordance with the principles of Articles 5, 6 and 25 of the GDPR).
- Only use customer data for the purpose it was collected and in accordance with MOBILITAS's privacy policy
- Report all policy violations to: DataProtectionOfficer@mobilitas.org

Users shall not:

- Copy or store sensitive/proprietary information or customer information on removal media devices
- View material that is: sexually explicit, profane, obscene, harassing, fraudulent, racially offensive, defamatory, or otherwise unlawful in nature
- Download material or software from the internet or unknown sources

- Install software on MOBILITAS systems or equipment
- Modify, revise, transform, or adapt any MOBILITAS software install on equipment and systems
- Transfer MOBILITAS or MOBILITAS customer data through any unsecure network, (in accordance with the principles of Articles 5, 6 and 25 of the GDPR).
- Use any utility program which allows the circumventing of MOBILITAS applied controls
- Send unsolicited emails or send spam emails
- Use MOBILITAS systems or equipment for any activity that violates local, state, federal, or international law
- Introduce any malicious software (virus, trojan, malware, etc.) into or onto MOBILITAS systems or equipment
- Use MOBILITAS equipment or systems in support of "for-profit" activities or outside employment/business activity (such as consulting for pay, sale of goods, etc.)
- Use MOBILITAS systems or equipment for malicious activities
- Acquire, use, reproduce, transmit, or distribute any controlled information including computer software and data that includes information subject to the Privacy Act, copyrighted, trademarked or material with other intellectual property rights (beyond fair use), proprietary data, or export-controlled software or data
- Remove MOBILITAS systems or equipment from the organization without prior management approval
- Post information on social media sites or other public forums which: are derogatory to MOBILITAS or its management, contrary to MOBILITAS's code of conduct and mission, or brings discredit to MOBILITAS, (in accordance with the principles of Articles 5, 6 and 25 of the GDPR).

b. Data Retention (in accordance with the principles of Articles 5, 6 of the GDPR).

Information created, received, or maintained in the transaction of MOBILITAS business, whether in paper or electronic form, is considered a formal record and is subject to MOBILITAS's Control of Record Procedure. This procedure defines the process for identification, storage, protection, retrieval, retention, hold, and disposition of records.

MOBILITAS will not keep personal information in a form that permits identification of data subjects for longer than necessary for the purposes for which it was collected or to which the data subject has consented, except for legitimate purposes permitted by law, such as regulatory compliance. All record disposals will follow MOBILITAS Derelict Media Collection and Destruction Process.

c. Remote working

When applicable, employees working remotely should follow the Remote Working policy and take additional precautions to ensure the protection of data by properly securing, both logically and physically, all equipment, data, and communications. Remote work can only be done on company provided equipment and in no case use of personal equipment.

d. Artificial Intelligence (AI) (in accordance with the principles of Articles 5, 6 and 25 of the GDPR).

Artificial intelligence (AI) tools are transforming the way we work. They have the potential to automate tasks, improve decision-making, and provide valuable insights into our operations, (in accordance with the principles of Articles 5, 6 and 25 of the GDPR).

However, the use of AI tools also presents new challenges in terms of information security and data protection. Regulations allow for an ethical and seamless evolution of artificial intelligence (AI). Its integration into our functional processes required strict compliance with Data Protection regulations. We have reconciled Artificial Intelligence (AI) and Data Protection, which implies that any collection and use of personal data by AI systems respects the rights of individuals and guarantees their security, this implementation was done within the framework of Privacy by design. These included the principles of fairness and transparency of processing, and the exercise of the rights of individuals over their data, (in accordance with Article 32 of the GDPR).

The use of AI for data protection requires diligent management to ensure compliance with regulations and enhances the security of personal information collected and processed. Mobilitas has robust security measures in place to prevent risks related to the use of AI, particularly in terms of cybersecurity. This includes protection against data leaks and potential cyberattacks, (in accordance with the principles of Articles 5, 6 and 25 of the GDPR)..

This policy requires full adherence and implies that all employees use AI tools in a manner that is consistent with our security best practices, (in accordance with the principles of Articles 5, 6 and 25 of the GDPR).

This section is a guide for employees on how to be safe when using AI tools, especially when it comes to sharing potentially sensitive company and customer information, (in accordance with the principles of Articles 5, 6 and 25 of the GDPR).

These regulations promote the homogenization of practices, facilitate adoption for a better acceptance and for a perfect integration of AI in the group. To do this, the establishment of a common culture requires us to identify the purposes allowing the use of AI tools by our employees, (in accordance with the principles of Articles 5, 6 and 25 of the GDPR).:

1) Generative AI, tools that help automate repetitive processes and optimize operational efficiency such as ChatGPT and Vidyo.ai facilitate communication and task management based on learning models, (in accordance with the principles of Articles 5, 6 and 25 of the GDPR).
2) Data Analytics, Tools to help analyze and interpret business data for more informed decisions, (in accordance with the principles of Articles 5, 6 and 25 of the GDPR).

Under the control of dedicated teams

3) Content generation, Tools that allow you to create content for the improvement of marketing communication are exclusively reserved for the teams in charge of communication within the group.
4) Infrastructure security remains under the control and sole responsibility of the IT department.

In addition, all employees should adhere to the following security best practices when using AI tools, (in accordance with the principles of Articles 5, 6 and 25 of the GDPR):

a. Evaluating AI tools: IT should assess the security of all AI tools before approving their use. This includes reviewing the tool's security features, terms of use, and privacy policy. They should also check the reputation of the developer of the tool and the third-party services used by the tool.

b. Protection of Confidential Data: Employees must not upload or share confidential, proprietary, or legally protected data without prior approval from the appropriate department. This includes data relating to the company, customers, employees or partners.

c. Access Control: Employees must not provide access to AI tools outside the company without prior approval from the appropriate department or manager and subsequent processes required to meet security compliance requirements. This includes sharing login credentials or other sensitive information with third parties, (in accordance with the principles of Articles 5, 6 and 25 of the GDPR).

d. Use of reputable AI tools: Employees should only use reputable AI tools and be careful when using tools developed by people or companies without an established reputation. Any AI tool used by employees must meet our security and data protection standards, (in accordance with the principles of Articles 5, 6 and 25 of the GDPR).

e. Compliance with security policies: Employees should follow the same security best practices that are used for all company and customer data. This includes using strong passwords, updating software, and adhering to data retention and disposal policies, (in accordance with the principles of Articles 5, 6 and 25 of the GDPR).

f. Data Privacy: Employees should exercise discretion when sharing information publicly. Personal information should not be used in an AI tool that may use this data publicly, (in accordance with the principles of Articles 5, 6 and 25 of the GDPR).

12. Supplier management

a. Vendor Management

Vendors, third parties, and supply chain partners will be held to the same standards contained within MOBILITAS's Data Security Policy, Privacy Policy and Code of Conduct. Additionally, they may be required to meet customer contractual controls if/when processing customer data. Audits will be conducted on these parties as applicable to ensure compliance is met and the required protections are provided. Relationships with vendors, third parties, and supply chain partners will be governed by mutually accepted contractual requirements, (in accordance with the principles of Articles 5, 6 and 25 of the GDPR).

b. Software and systems procurement

The procurement of new systems and software will follow a defined process to ensure an unbiased and comprehensive review of offering is conducted prior to purchase. The review process will specifically include a data security review to ensure the offering has appropriate security controls and features, (in accordance with the principles of Articles 5, 6 and 25 of the GDPR).

Appendix 1: Data Classification and Handling

All information assets are assigned a sensitivity level based on the data element's level of sensitivity, value, and criticality to MOBILITAS, its customers, agents, contractors, or business partners.

CLASSIFICATION	DATA CLASSIFICATION DESCRIPTION	
CONFIDENTIAL	Definition	Highly sensitive information that requires the highest level of protection. This includes financial data, personally identifiable information (PII), intellectual property, and trade secrets.
	Potential Impact of Loss	**CRITICAL DAMAGE** would occur if Highly Restricted information were to become available to unauthorized parties either internal or external to MOBILITAS. Impact could include negatively affecting MOBILITAS's competitive position, violating regulatory requirements, damaging the company's reputation, violating contractual requirements, and posing an identity theft risk.
MANAGER	Definition	Business, strategic or organizational Information meant only for senior employees such as branch managers, network managers, board members.
	Potential Impact of Loss	**HIGH DAMAGE** would occur if Manager information were to become available to unauthorized parties either internal or external to MOBILITAS. Impact could include negatively affecting MOBILITAS's competitive position, damaging the company's reputation, violating contractual requirements, and exposing the geographic location of individuals.
INTERNAL	Definition	Information meant for internal use within the organization. Access is limited to authorized personnel and includes data like policies, internal communications, and non-sensitive reports.
	Potential Impact of Loss	**MODERATE DAMAGE** would occur if Restricted information were to become available to unauthorized parties either internal or external to MOBILITAS. Impact could include negatively affecting MOBILITAS's competitive position, damaging the company's reputation, violating contractual requirements, and exposing the geographic location of individuals.
SUPPLIER	Definition	Information intended to be shared but only with suppliers for them to complete the services they need to provide to the group. Examples include working rules, specific login details, operational data.
	Potential Impact of Loss	**MODERATE DAMAGE** would occur if Restricted information were to become available to unauthorized parties either internal or external to MOBILITAS. Impact could include negatively affecting MOBILITAS's competitive position, damaging the company's reputation, violating contractual requirements, and exposing the geographic location of individuals.
EXTERNAL	Definition	Information intended for public disclosure without any restrictions. Examples include marketing materials, press releases, and general company information.
	Potential Impact of Loss	**NO DAMAGE** would occur if public information were to become available to parties either internal or external to MOBILITAS. Impact would not be damaging or a risk to business operations.