CAP4GROUP

Systems & Information Security

Information Security External Statements

Cap4Group presents this quality assurance plan as a commitment to customers, partners, and other stakeholders, underscoring the dedication to maintaining confidentiality, integrity, availability, and resiliency in the processing and management of systems and information.

This document details the approach to embedding these core principles into services and operations, aimed at promoting a high level of trust and customer satisfaction in information security.

CAP4GROUP

Table of Contents

Introduction

In an era where data protection has become imperative for any entity operating in the digital space, Cap4Group is resolutely invested in establishing a secure environment for its operations. This approach aims to preserve and strengthen the trust of its customers.

Recognizing the critical importance of information security, Cap4Group is committed to adopting and implementing robust security strategies that are responsive to the evolving challenges and threats of today's digital landscape.

The goal is to ensure the integrity, confidentiality and availability of the data processes, aligning the practices with the highest international standards.

This security assurance plan is the foundation of the commitment to providing a secure working environment and customer service that meets the highest expectations for IT security.

Scope

This security assurance plan details Cap4Group's internal security practices, as well as the specific security measures implemented when implementing solutions for the customers and as part of maintenance services. It encompasses three key areas:

1. Internal Security Practices

This section focuses on Cap4Group's internal policies, procedures, and security measures. It includes access management, employee security awareness, securing internal infrastructure and data, and managing security incidents.

2. Security during the implementation of solutions

Here, we discuss the security approaches and standards applied during the design, development and deployment of solutions for the customers. This includes risk assessment, integrating security by design, as well as tailoring security measures to each customer's specific context.

3. Maintenance Services

This section describes the procedures and security measures used to maintain the security of solutions after deployment. It covers continuous monitoring, system updates to fix vulnerabilities and technical support that may occur during the operational life of the solutions.

The purpose of this plan is to detail the consistent and integrated framework that ensures the security of Cap4Group's information and systems, while supporting the trust and satisfaction of the customers.

Security Actors

The implementation of a secure framework within Cap4Group relies on the commitment and well-defined responsibilities of several key stakeholders, including the customers. These individuals and groups play a crucial role in information security governance, ensuring that security strategies, policies, and procedures are properly developed, enforced, and maintained. The main security players within Cap4Group include:

1. Management

Management commitment is fundamental to establishing the importance of information security within the organization. It provides the necessary resources, defines the security vision and objectives, and ensures that information security is aligned with the company's strategic objectives. Management also supports the culture of security across all layers of the organization.

2. The CISO (Chief Information Security Officer)

The CISO is responsible for overseeing the information security strategy and its implementation across the organization. As the primary security policy architect, he is the point of contact for all information security matters, working closely with the various departments to mitigate security risks. He also promotes a culture of information security within the organization, manages cyber incidents and crises and governs day-to-day activities to protect IT systems.

3. The DPO (Data Protection Officer)

Focused on the protection of personal data, the DPO ensures the organization's compliance with data protection laws and regulations. It raises awareness and trains staff on data protection obligations and serves as a point of contact with regulatory authorities.

4. Collaborators

All employees, regardless of their role or position, are considered security actors. They need to be aware of their role in protecting the company's information assets, hence the importance of ongoing training and awareness.

5. Customers

Customers also play a vital role in Cap4Group's secure framework. Their feedback is essential to identify potential security vulnerabilities and improve protection measures. Cap4Group encourages open communication with its customers to receive their opinions and suggestions regarding the security of the solutions provided. This collaboration allows security practices to be continuously adapted and refined to best meet customer needs and expectations.

Each of these actors contributes in an indispensable way to the construction and maintenance of a secure framework within Cap4Group.

Regulatory framework and security standards

Cap4Group navigates a complex global environment, subject to various regulatory frameworks and security standards depending on the territories where the company operates. Regulatory compliance is paramount in the security strategy to ensure both data and system protection, as well as compliance with jurisdiction-specific legal obligations.

1. Regulatory framework

Operating in regions such as the European Union, Luxembourg, Germany, France, Italy, Switzerland, Hong Kong, Shanghai, and Portugal, Cap4Group is subject to local laws and regulations regarding data protection and information security.

The General Data Protection Regulation (GDPR) stands out as a key regulation for the activities within the EU and EEA, imposing strict guidelines for the management and protection of personal data.

2. Security Standards:

Cap4Group is committed to internationally recognized security standards, including, among the others, ISO/IEC 27001, 27002, 27005 and ISO/IEC 27701. In preparation for upcoming ISO certification, ensuring a high level of information security, Cap4Group is working to align its security policies, procedures, and controls with these standards.

In addition to ISO 27001, we leverage on several other security standards that are widely recognized and used as benchmarks in the information security world.

a) ISO/IEC 27001

Provides a framework for Information Security Management Systems (ISMS), helping Cap4Group secure assets such as financial information, intellectual documents, employee personal data, or information entrusted by third parties.

b) ISO/IEC 27002

Provides a set of best practices for information security management, guiding Cap4Group in implementing effective security controls to address information security risks.

c) ISO/IEC 27005

Focuses on information security risk management, providing guidance for assessing, addressing, and monitoring information security risks within an organizational framework.

d) ISO/IEC 27701

Extends the principles of ISO/IEC 27001 and 27002 to the management of personal data protection. This standard is particularly relevant to Cap4Group in the context of the GDPR, as it provides guidelines for a Privacy Management System (PIMS), helping to manage privacy risks and strengthen data protection compliance.

e) NIST Cybersecurity Framework

A framework developed by the National Institute of Standards and Technology (NIST) in the United States, which provides a structure for managing and reducing cyber risk.

f) ISF Standard of Good Practice for Information Security (SOGP)

SOGP presents business-orientated information security topics with practical and trusted implementation-level guidance. Covering a wide range of information security topics that are relevant for current and emerging threats, technology and risks, its broad scope and extensive guidance enables organisations to integrate up-to-date good practice with their business processes, information security programme, risk management, and compliance arrangements.

Security Governance

To ensure effective information security governance, Cap4Group has established a comprehensive set of documents governing the various aspects of its security strategy. These documents serve as the foundation of data protection and IT security risk management. Here is an overview of the key documents that make up the security governance framework:

IT Charter

Serves as a preamble to the approach to IT security, establishing the company's guiding principles and commitment to information systems security.

Information Security Policy

Defines the overall objectives, scope and responsibilities for information security within Cap4Group.

Asset Management Policy

Details procedures for effective management of information assets, ensuring their protection throughout their lifecycle.

Acceptable Use Policy

Sets out permitted and prohibited behaviors regarding the use of company IT resources, aimed at preventing abuse and security risks.

Identity and Access Control Policy

Specifies identity and access management rules to ensure that only authorized individuals can access sensitive information.

Password Policy

Establishes requirements for creating, managing, and securing passwords, which are essential to protect access to systems and data.

Cryptography Policy

Describes the use of cryptographic technologies to protect the confidentiality, integrity, and authenticity of information.

Physical Access Security Policy

Addresses securing physical access to corporate facilities to protect against unauthorized access.

Personnel Security Policy

Balances personnel security aspects, including but not limited to employee recruitment and departure.

Secure Development Policy

Guides secure development practices to ensure software and systems are designed with security.

Change Management Policy

Provides a framework for the management of changes on information systems to minimize the associated security risks.

Patch Management Policy

Defines the security update management strategy for software and systems, which is essential for remediating vulnerabilities.

Business Continuity Plan

Sets out the procedures to be followed to ensure the continuity of operations in the event of a major incident affecting Cap4Group.

Backup Policy

Establishes guidelines for the regular backup of critical data, including methods, frequency, and secure storage of backups to ensure effective recovery in the event of a disaster.

Security Incident Response Policy

Establishes the process for managing security incidents, from identification to resolution, to notification of relevant parties.

Third-Party Security Policy

Defines security requirements for third-party partners and vendors, ensuring that their practices comply with Cap4Group standards.

Homeworking Policy

Adapts security principles to the work-from-home environment, addressing the specific challenges of off-premises security.

Risk Management

Risk management is a fundamental pillar of Cap4Group's information security strategy. The systematic and proactive approach aims to identify, assess, and mitigate information security risks that may affect the assets, operations, or stakeholders, according to ISO/IEC 27005 : Information security risk management and NIST Cybersecurity Framework.

1. Risk Identification

The first step in the risk management process is to comprehensively identify potential risks that could compromise the confidentiality, integrity, or availability of the information and systems. This identification is based on continuous analysis of the internal and external environment, using proven tools and methodologies to detect potential threats and vulnerabilities.

2. Risk assessment

Once risks have been identified, they are assessed based on their likelihood of occurrence and the potential impact on the organization. This assessment makes it possible to classify risks into categories, determine their level of criticality and prioritize mitigation actions.

3. Risk Mitigation

Based on the risk assessment, mitigation strategies are developed and implemented to reduce the likelihood of risk occurrence or minimize the impacts of risks. These strategies may include adopting new security policies, strengthening technical controls, training employees, or modifying organizational processes. Each mitigation action is carefully planned, executed, and monitored to ensure its effectiveness.

4. Risk monitoring and review

Risk management is a dynamic process that requires regular monitoring and reassessment. Cap4Group is committed to monitoring the security environment to detect any changes in the risk profile, requiring an adaptation of mitigation strategies. Periodic reviews are conducted to assess the effectiveness of control measures and to identify new emerging risks.

5. Risk communication and reporting

Effective communication is essential to ensure successful risk management. Cap4Group ensures that relevant information on security risks is appropriately communicated to all levels of the organization, as well as to external stakeholders when necessary. Regular reports are prepared to inform management of current risks, mitigation measures in place, and the overall effectiveness of the risk management process.

Security Incidents

Security incident management is a critical part of the overall information security strategy. It aims to identify, respond to, contain and recover from any security incident in an efficient and organized manner, thereby minimising the impact on operations and on the confidentiality, integrity and availability of the data processed. This chapter, which is inspired and follow de facto security standards as ISO/IEC 270035 and NIST Cybersecurity Framework, describes the structured approach to managing security incidents within the organization.

1. Preparation

The first line of defense against security incidents is robust preparedness, which includes training employees, setting up incident detection systems, creating an incident response plan and the escalation process, defining roles and responsibilities and implementing security tools and technologies. All employees receive regular training on how to recognize the signs of security incidents and how to report them.

2. Identification

Rapid identification of security incidents is crucial for an effective response. Cap4Group has monitoring systems and alerts in place to detect any abnormal or suspicious activity on the network and systems. If a potential security incident/threat is detected, the security team is immediately alerted to assess the situation.

3. Answer

Once an incident is identified, the incident response team follows an established plan to contain, eradicate, and recover from the incident. This plan includes specific procedures for:

a) Containment

Take immediate action to limit the scope and impact of the incident.

b) Eradication

Identify and eliminate the cause of the incident to prevent its recurrence.

c) Restoration

Restore affected systems and data to their normal operating state in a secure manner.

4. Communication

Communication is an essential aspect of incident management. Cap4Group is committed to communicating transparently and in a timely manner with all relevant stakeholders, including customers, employees and, if necessary, regulatory authorities when the incident involves personal data or if it poses a significant risk to customers' business. This communication includes information on the nature of the incident, the actions taken in response and recommendations for the affected parties.

5. Post-Incident review

After an incident is resolved, a post-incident review is conducted to assess how the incident was handled and to ascertain root cause, update playbooks and incident response plan based on the lesson learned from the incident. The goal is to continuously improve incident response processes and strengthen security measures to prevent future incidents.

6. Details: Personal Data Breaches

In the event of a personal data breach, close coordination between the Data Protection Officer (DPO) and the Chief Information Security Officer (CISO) is essential for effective incident management.

The DPO and CISO work together to ensure that all legal obligations are met, including notification to supervisory authorities and, affected individuals or the client if Cap4Group is acting as a processor, in accordance with the requirements of the GDPR. This collaboration ensures that the response to the incident is not only technical but also compliant with data protection requirements, minimizing legal and reputational impacts for the organization.

Security incident management is an ongoing and evolving process. Cap4Group is committed to investing in best practices, technology, and training to ensure operations remain secure and resilient in the face of ever-evolving threats.

Internal Security Practices

1. User Awareness Management

Cultivating a culture of security across the organization requires ongoing user awareness and training. With a focus on personal data protection and security best practices, Cap4Group strengthen the first line of defense against cyber threats.

a) Annual Data Protection Training

Cap4Group engages its teams in a continuous learning process on the protection of personal data. This translates into annual trainings to ensure that each member fully understands the implications and responsibilities involved in handling this data.

b) Security Best Practices Training

As IT security is constantly evolving, Cap4Group holds regular training sessions to keep the staff up to date on the latest threats and relevant defense strategies. These trainings strengthen the security culture within the organization.

c) Monthly Awareness

Cap4Group sends monthly emails to make people aware of punctual, company-related security topics.

d) Security incident simulation

The organization implements tabletop security incident simulations with the participation of managers and stakeholders. This discussion-based exercise involves role-playing through a simulated security scenario, enabling organizations to prepare for and effectively respond to real security incidents.

2. Identity and Access Management

IAM is pivotal in managing digital identities and regulating their access to IT resources. This framework supports Cap4Group by guaranteeing that the appropriate individuals gain access to the necessary resources precisely when needed, thereby enhancing our overall security posture and compliance with regulatory requirements.

a) User Authentication Management

Authentication plays a crucial role in securing access to systems and information. By assigning unique logins and requiring strong and regularly renewed passwords, Cap4Group ensures a high level of protection against unauthorized access.

1. Personal and Unique Identifiers

Cap4Group assign each user a unique identifier, eliminating the need for generic identifiers and improving security and traceability within systems.

2. Password security and management

The password policy imposes strict criteria: for users, a password of at least 10 characters including numbers, lowercase letters, uppercase letters and special characters. For privileged accounts, this requirement is increased. Cap4Group also applies two-factor authentication on different systems to enhance access security. Passwords are regularly renewed, and their reuse is prohibited, even during the first login, to ensure optimal security.

3. Throttling logging attempts

Cap4Group have a mechanism in place to limit failed login attempts. If the allowed number of trials is exceeded, a specific procedure is activated to secure the affected account and investigate the incident. This preventative measure is crucial to counter brute force attacks.

b) User Permissions Management

Accurate assignment of access rights is essential to limit the exposure of sensitive data. By applying the principle of least privilege through role-based authorization profiles, Cap4Group minimizes the risk of data leakage while facilitating access management.

1. Role-based authorization profiles

Cap4Group define precise authorization profiles, based on the roles and responsibilities of each user within the company. This approach, known as Role-Based Access Control (RBAC), ensures that access to data and systems is strictly limited to what is necessary for the user's functions.

2. Removing Deprecated Permissions

Permissions that have become obsolete, whether by changing positions or tasks, are immediately deleted. A clear process is in place to quickly inform administrators of the need for this deletion, ensuring that only authorized personnel have access to critical resources.

3. Annual Review of Authorizations

To maintain an optimal level of security, Cap4Group conduct an annual review of all access permissions. This process helps identify and rectify any inappropriate or outdated permissions, ensuring that access remains strictly necessary and relevant.

3. Event Logging

Logging actions performed on systems provides essential traceability in the event of a security incident. This information gathering is vital for event analysis, incident response, and compliance audits.

a) Logging Systems

Advanced logging systems are in place to record user activities, including system access, as well as data creation, read, modification, and deletion actions. This traceability is essential for analyzing security incidents and for compliance audits.

b) Logging Information

All users are informed of the existence and purpose of the logging systems. This transparency aims to increase awareness of the importance of security and compliance with policies for the use of information systems.

c) Securing Recording Systems

Special security measures protect recording systems against unauthorised access and manipulation. Ensuring the integrity and confidentiality of event logs is crucial for reliable analysis in the event of an incident.

4. Workstation Management

Securing workstations is fundamental to protecting information from unauthorized physical and virtual access. Measures such as automatic locking of idle sessions and the Clean Desk policy contribute to this security.

a) Auto-lock procedure

Cap4Group has implemented a procedure for automatically locking sessions on workstations after a period of inactivity. This practice helps prevent unauthorized access to unattended desktops, thereby increasing the security of corporate data and resources.

b) Clean Desk Policy

The Clean Desk policy has been formalized to encourage employees to keep their workspaces clear of sensitive documents and removable media when they are not present. This reduces the risk of accidental exposure of confidential or sensitive information.

c) Consent for maintenance interventions

Before any intervention on workstations or other devices not managed by maintenance personnel, the user's consent is required. This approach ensures that users are informed of and agree with the actions taken on their systems, contributing to the transparency and security of maintenance operations.

5. Mobile Computing Management

Mobility brings with it specific security challenges. By encrypting data on mobile devices and establishing clear guidelines for its use, Cap4Group maintain the confidentiality and integrity of information, even when it's out of the office.

a) Mobile Device Encryption

Cap4Group require encryption of all mobile devices used in the workplace. This critical security measure protects corporate information stored on these devices in the event of loss or theft.

b) Device Unlock Guidelines

Clear guidelines have been established regarding methods of unlocking mobile devices, ensuring that only authorized users can access corporate data on these devices.

c) Safe to use in public places

Cap4Group has formalized rules regarding the use of mobile computing in public places, aimed at reducing security risks such as shoulder surfing and unsecured access to public Wi-Fi networks.

6. Internal management of the network and the Internet network

Protecting the internal network and internet access is crucial to defend the organization against external attacks. Installing firewalls, implementing antivirus software, and network segregation are among the key strategies for securing the network infrastructure.

a) Installing and Configuring Firewalls

Firewalls are installed and configured to monitor and control incoming and outgoing traffic according to a defined security policy. This barrier helps protect the internal network and Cap4Group devices from unauthorized access and external attacks.

b) Antivirus Software Deployment

Anti-virus software is installed on all devices in the information system and is regularly updated. This preventative measure plays a crucial role in protecting against malware and other malware.

c) Wi-Fi Network Security

Wi-Fi networks are secured with proper security protocols, and access requires authentication. This approach prevents unauthorized access and ensures the protection of wireless communications within the enterprise.

7. File Systems and Database Management

The security of stored data is based on the implementation of rigorous access controls and the regular performance of vulnerability scans. These practices help prevent unauthorized access and ensure data integrity.

a) Critical Updates

Critical system and application updates are prioritized and applied without delay. By staying up-to-date with the latest security patches, Cap4Group minimizes windows of exposure to known vulnerabilities and strengthen the overall security posture.

8. Web Platform Management

Web platforms are common attack vectors. By adopting practices such as the use of TLS to encrypt transmitted data and conducting regular security scans, Cap4Group ensures the security of web interfaces.

a) Regular vulnerability scans

Web interfaces undergo regular vulnerability scans to detect and remediate potential security vulnerabilities. These systematic assessments ensure that web platforms are robust and protected against online attacks.

b) Implementing TLS 1.2 or higher

To secure communications on web platforms, Cap4Group implements TLS 1.2 or higher. This ensures that data transmitted between web servers and users' browsers is encrypted and secure, protecting against eavesdropping and data modifications.

c) HTTPS Certificates

All of web platforms are equipped with HTTPS certificates, ensuring visitors have a secure and authenticated connection. This practice strengthens users' trust in services and helps to secure the exchange of sensitive information.

d) Compliant cookie management

The management of cookies on web platforms complies with the GDPR. Cap4Group obtain explicit consent from users before any non-essential cookies are placed and provide clear information on the use of cookies, thus enhancing the respect for the privacy of visitors.

e) OWASP Type Controls

Cap4Group apply security controls based on OWASP recommendations for web interfaces, aimed at preventing common vulnerabilities in web applications. These controls include protection against SQL injections, authentication security breaches, and cross-site scripting (XSS) flaws, among others.

9. Backup & Synchronization Management

Regular and secure backups help ensure data availability even in the event of an incident. Encryption of backups ensures that these copies cannot be exploited by unauthorized third parties.

a) Regular backups and synchronizations

Regular backups and data synchronizations are performed to ensure the availability and integrity of business information. These operations are

essential for data recovery in the event of a security incident or technical failure.

b) Backup Isolation

Backups are carefully isolated from production information systems and stored in secure, geographically separated locations. This diversification strategy strengthens the ability to restore operations quickly in the event of a major disaster.

c) Encryption of backups

For maximum security, all backups are systematically encrypted. Encryption ensures that even in the event of unauthorized physical access to backup media, data remains protected and inaccessible without the proper decryption keys.

10. Information Archiving

Secure archiving of data allows for long-term preservation while ensuring controlled access. The proper destruction of archives follows defined retention periods, in compliance with legal and organizational requirements.

a) Specific access to the archives

Cap4Group has put in place specific access arrangements for archived data, ensuring that this information, although no longer used on a daily basis, remains protected and accessible only by authorized users. This helps to maintain the integrity and confidentiality of the archives over the long term.

b) Compliant Destruction of Records

The destruction of archives follows defined retention periods and complies with regulatory and organizational requirements. Cap4Group uses secure destruction methods to ensure that data cannot be recovered or reconstructed, protecting sensitive information even at the end of its life.

11. IT Development Management

Integrating security by design and throughout the development lifecycle of IT systems is essential. This approach, coupled with rigorous security testing, ensures the creation of reliable and secure solutions.

a) Separation of environments

Cap4Group has implemented a strict separation between development, test, and production environments. This preventative measure prevents cross-contamination and ensures that unverified changes do not compromise the production environment. It also eases the debugging process and improves the overall security of the system.

b) Definition of security requirements

Before the start of any project, Cap4Group clearly defines the security requirements for the developments to be undertaken. This includes secure coding standards, communication protocols to be used, and access control mechanisms, ensuring that every aspect of development is guided by robust security principles.

c) Post-implementation checks

After each implementation, detailed checks are performed to ensure that new features or changes do not introduce vulnerabilities within the system. This step includes penetration testing, code reviews, and security audits.

d) Security requirements for applications

All applications used in development are subject to a prior security assessment. This ensures that only applications that meet security standards are used, reducing the risk of exposure to third-party vulnerabilities.

e) Security by Design & by Default

Cap4Group takes a «Security by Design & by Default» approach to all new systems. This means that security is built into the first design phase and the default security settings are as restrictive as possible, minimizing the potential attack surface.

f) Zero Trust and Always Verify

The security philosophy is based on the principle of «Zero Trust», where no entity is considered secure by default, and all must be constantly verified. This applies to all users, devices and networks, ensuring a heightened level of security through systematic verification.

g) Assume Breach

Cap4Group takes the «Assume Breach» approach in the security management, which means that Cap4Group operates as if a security breach has already

occurred. This perspective drives the entity to put in place robust incident detection and response measures to respond quickly and effectively in the event of an attack.

h) Principles of Secure Development

Development activities are rigorously guided by secure development principles, including the creation of secure architectures, adherence to coding standards, and the use of controlled environments. Cap4Group also makes sure to make developers aware of practices that have led to vulnerabilities in the past.

Please note that in contractual relationships, Cap4Group *strictly follows clients security guidelines. Clients must define them and inform* Cap4Group *of development security measures wanted.*

i) Dedicated Security Testing

Before going into production, the developments are subjected to rigorous tests in dedicated environments. These tests cover functional security, code security, and configuration security, ensuring that new developments are robust and secure.

j) Change Management

Any change, whether hardware, software, or configuration, is subject to a rigorous change management process. This process includes planning, authorization, communication, and documentation, ensuring that each change is made in a controlled and secure manner.

k) Anonymization of test data

Data used in test and development environments is anonymized to prevent accidental exposure of sensitive information. This practice ensures that personal or confidential data is not compromised during the development process.

Please note that it is the customer's responsibility to transmit an anonymized or fictitious database to Cap4Group *or to ask the organization to anonymize the data. The organization will consider any external database to be outside the scope of the GDPR unless otherwise specified.*

12. Hardware and software maintenance and end-of-life

Secure maintenance and end-of-life management of IT assets is crucial to avoid vulnerabilities. Clear processes for secure data erasure and hardware recycling help protect the organization from security risks.

a) Documentation of maintenance interventions

All maintenance interventions on systems are carefully documented, providing a complete history of changes, updates and repairs made. This transparency helps maintain the security and stability of the IT infrastructure.

b) Secure data erasure

When hardware or software reaches its end of life, Cap4Group securely erases the data it contains. This critical step ensures that sensitive information is irretrievable before the material is recycled, transferred, or destroyed.

13. Third-party management

Managing third parties, including processors, is a crucial aspect of the security and compliance strategy, particularly with respect to compliance with the General Data Protection Regulation (GDPR).

Particular attention is paid to the selection, engagement and monitoring of processors to ensure that they adhere to the same high standards of data protection as Cap4Group sets itself. This section details the approach to managing GDPR processors and the steps Cap4Group takes to ensure compliance.

a) GDPR processors

GDPR processors are partners or service providers who may have access to personal data for which Cap4Group acts as a controller or processor for customers, these processors are then referred to as sub-processors.

The key distinction here is that these entities process personal data on Cap4Group behalf, requiring rigorous management and compliance with GDPR requirements.

To ensure this compliance, Cap4Group takes the following steps:

4. GDPR-specific clauses in contracts

All contracts with processors include clauses specific to the GDPR and which require compliance with the security measures mentioned

in this document, at least if the processor does not have certifications to ensure that the technical and organizational measures put in place in terms of information security are sufficient.

5. Conditions for return and destruction of data

The contracts clearly stipulate the conditions under which personal data must be returned or destroyed at the end of the service. This ensures that no personal data remains in the possession of processors once their need for access is over.

6. Verification of the effectiveness of contractual guarantees

To ensure that subcontractors meet their contractual obligations, Cap4Group conducts regular audits when they do not have adequate certifications. This may include security audits, site visits, and annual due diligence. These assessments make it possible to verify the effective application of security measures and compliance with contractual conditions.

7. Monitoring of Processors' Activities

Where possible, the activities of subcontractors are monitored by one or more members of the organization. This continuous monitoring ensures that subcontractors maintain the security and data protection standards required by the policy and by the legislation in force.

14. Management of internal and external communication

Securing communications involves encrypting data exchanges and verifying the trustworthiness of recipients, thus protecting against information leakage and interception.

a) Encrypt data in transit

To protect the integrity and confidentiality of the data exchanged, both internally and with external parties, Cap4Group encrypts data in transit. This preventative measure is essential to prevent interception and unauthorized access during the transfer of sensitive information.

b) Recipient Reliability

Before any transfer of sensitive information or supporting documents, Cap4Group takes steps to verify the trustworthiness of the recipients. This includes validating identity and confirming data access permission, reducing the risk of disclosure to unauthorized parties.

c) Preventing Unauthorized Transfer

Cap4Group has established procedures to prevent the unauthorized transfer of sensitive documents, including credentials. In the event of an absolute necessity for a transfer, Cap4Group uses multiple and secure communication channels, such as the sending of protected PDF files, to enhance the security of the exchange.

15. Premises Management

The physical security of the premises plays a complementary role to IT security. Measures such as alarm systems and video surveillance are essential to protect physical and IT assets, according to local laws and regulations.

a) Enhanced physical security

The security of premises is ensured by advanced locking systems, limiting access to sensitive areas to authorized personnel. This physical barrier is complementary to IT security measures and plays a crucial role in protecting the infrastructure and data.

b) Installation of alarm and video surveillance systems

To prevent intrusions and monitor activities around and inside premises, Cap4Group has implemented alarm and video surveillance systems. These deterrents and controls contribute to continuous monitoring and rapid response in the event of a security incident.

c) Protection against environmental damage

Cap4Group takes measures to protect against environmental damage, such as floods, fires, and other natural or man-made disasters. This includes the use of resilient materials, the establishment of early warning systems, and business continuity planning to ensure operational resilience.

16. Encryption Management

Encryption is a fundamental security measure to protect data privacy. Rigorous management of encryption keys is necessary to maintain the effectiveness of this protection over time.

a) Updating Encryption Algorithms

Aware of the constant evolution of threats and decryption techniques, Cap4Group ensures that the encryption algorithms used are regularly updated according to current security standards. This technology watch ensures effective protection of sensitive data, both at rest and in transit.

b) Secure encryption key management

The management of encryption keys is carried out with special care to ensure their security and integrity. This includes secure storage, limiting access to keys, and renewal and revocation procedures to respond quickly to any security incidents.

Security during the implementation of solutions

Cap4Group's approach to security when implementing solutions at customers' premises is based on close collaboration and transparent communication with each customer.

This critical phase of the process requires careful attention to ensure that the customer's systems and data remain protected throughout the integration.

1. Collaboration on risk assessment

The first step in any implementation involves a joint assessment of risks specific to the customer's environment. Working together, Cap4Group identifies potential vulnerabilities within the client's existing architecture, business processes, and regulatory requirements.

This collaborative approach ensures that mitigation measures are fully aligned with the client's security needs and objectives.

2. Integration of security by design with the customer

Secure implementation starts long before the physical integration of solutions. In partnership with the customer, Cap4Group takes a «security by design» approach, ensuring that all solutions are pre-configured to incorporate security best practices tailored to the customer's specific environment.

This step includes securely configuring software, hardening systems, and implementing robust access controls.

3. Tailoring security measures to the customer's context

Recognizing that each customer has unique needs, Cap4Group tailors its security measures to specifically address each customer's operating context and security challenges.

This can include custom configurations or the implementation of specific security solutions.

4. Awareness

An integral part of the implementation process involves training and awareness of the client's teams. By providing awareness on the security

features of deployed solutions, Cap4Group helps strengthen the customer's overall security posture.

5. Post-implementation follow-up

After implementation, the commitment to security continues. Cap4Group can offer follow-up to ensure that solutions are working as intended in the customer's secure environment. This includes regular assessments, updates, and ongoing support to respond to any new threats or vulnerabilities.

Maintenance Services

Cap4Group's maintenance services offer useful support to maintain the security and efficiency of customers' systems after the implementation of the solutions. The approach is designed to be flexible, secure and tailored to each client's specific requirements.

1. Adaptive maintenance

Cap4Group understand that every customer has unique needs and availability for maintenance may vary. Based on this, Cap4Group offers adaptive maintenance services that can be programmed and customized according to each customer's specific operational requirements. This allows for maximum flexibility while ensuring that systems remain secure and efficient.

2. On-demand security updates and patches

Recognizing the critical importance of security updates and patches to protect against vulnerabilities, Cap4Group makes possible the management of these updates taking into account customers' preferences and availability. Cap4Group can perform on-demand security checks and deploy critical updates after consulting with the customer and planning interventions to minimize the impact on their day-to-day operations.

3. Monitoring

Depending on the arrangements agreed with the customer, Cap4Group can provide conditional monitoring of the systems to detect and alert on potential security issues. This monitoring is designed to be non-intrusive and respectful

of the confidentiality and integrity of the customer's systems, while providing an additional layer of protection.

4. Assistance & support

The support team is ready to step in to provide security assistance and advice, whether it's for one-off questions or more complex issues that require further investigation. Cap4Group ensures that the support is responsive and informed, offering solutions based on industry best practices.

Audit & Due Diligence

Transparency and compliance are fundamental pillars of Cap4Group's approach to information security and data protection. Cap4Group understand that customers may have specific questions or require further clarification about the security assurance plan. With this in mind, Cap4Group is fully willing to participate in audit and due diligence processes to provide the necessary peace of mind and confidence to partners and customers.

1. Answers to specific questions

If the security assurance plan or standard documents do not seem complete or specific to customers' needs, Cap4Group is ready to answer detailed questions and provide additional information required. The goal is to ensure full transparency and demonstrate the commitment to data security and protection in a concrete and measurable way.

2. Customized Audit & Due Diligence

Recognizing that every organization has unique security and compliance requirements, Cap4Group welcomes and facilitates customized audits and due diligence processes conducted by clients or their authorized representatives. These assessments can be specifically tailored to examine relevant aspects of the security infrastructure, policies and procedures, ensuring that they meet specific customer standards and expectations.

3. Compliance with Article 28 of the GDPR

When Cap4Group acts as a data processor, in accordance with the General Data Protection Regulation (GDPR), the commitment to security and data protection is also covered by Article 28 of the GDPR. This means that Cap4Group strictly adheres to the requirements set out for processors, including the implementation of appropriate technical and organizational measures to ensure the security of the data processed. Cap4Group is committed to fully cooperating with customers to respond to any assessment, audit or inspection related to compliance with Article 28 and beyond, ensuring that personal data is processed in a secure and compliant manner.

In summary, Cap4Group is committed to providing a level of transparency and cooperation that builds the customers' confidence in the ability to protect their most valuable information. Cap4Group welcomes audits and due diligence as opportunities to demonstrate the commitment to security and compliance excellence.