Forship

Information Security Policy with Suppliers

TABLE OF CONTENTS

1. PURPOSE

The Information Security Policy with suppliers is the document that guides and establishes the Forship Group's corporate guidelines for protecting the company's information in its relationship with suppliers.

2. SCOPE

The guidelines set out here must be followed by all employees, as well as service providers, and apply to information in any medium.

3. RESPONSIBILITIES

Managers

- Demand compliance with the policy from its suppliers.
- Raising awareness among critical suppliers.
- Report any risk or deviation.

DTI - IT Department

- Assessing information security risks and due diligence on suppliers.
- Determine actions and controls.
- Assisting in the management of supplier changes and agreement terminations.

Information Security Committee

- Determine supplier relationship requirements.

4. EXECUTION SYSTEM

In general, information security requirements vary according to the type of contractual relationship that exists with each supplier and the goods or services delivered.

However, the following generally applies:

- Information security requirements and controls must be formally documented in a contractual agreement that can be part of or an addendum to the main agreement.
- Separate non-disclosure agreements (NDA) should be used when there is a more specific level of control over the confidentiality agreement.
- Due diligence must be exercised in the selection and approval of new critical suppliers before agreements are signed.
- The information security provisions in place at existing suppliers (where due diligence was not carried out as part of the initial selection) should be clearly understood and improved where necessary.
- Remote access by suppliers must be via approved methods that comply with our information security policies.
- Access to Forship Group information should be limited, where possible, according to clear business need.
- Basic information security principles such as least privilege, segregation of duties, and defense in depth must be applied.

- The supplier is expected to exercise adequate control over the information security policies and procedures used by subcontractors who play a role in the supply chain delivering goods or services to the Forship Group.
- The Forship Group will have the right to audit the information security practices of the supplier and, where appropriate, subcontractors.
- Incident management and contingency plans must be implemented based on the results of a risk assessment.
- Awareness training will be carried out by both parties to the agreement, based on the defined processes and procedures.

The necessary controls must be selected based on a comprehensive risk assessment, which considers the information security requirements, the product or service to be supplied, its criticality for the organization, and the supplier's capabilities.

4.1. DUE DILIGENCE

Before contracting a supplier, the Forship Group is responsible for conducting due diligence to gain as complete an understanding as possible of the company's approach to information security and the controls it has in place.

This is particularly important when cloud computing services are involved, as legal issues about the location and storage of personal data must be taken into account.

4.2. SECURITY IN AGREEMENTS WITH SUPPLIERS

Once a potential supplier has been positively assessed through due diligence, the Forship Group's information security requirements must be reflected in writing in the contractual agreement entered into. This agreement should consider the classification of any information to be processed by the supplier (including any necessary mapping between Forship Group classifications and those in use within the supplier), legal and regulatory requirements, and any additional security controls necessary.

For cloud service providers, information security roles, and responsibilities should be clearly defined in areas such as backups, incident management, vulnerability assessment, and cryptographic controls.

Appropriate legal advice should be obtained to ensure that the contractual documentation is valid in the country or countries in which it will be applied.

For those suppliers who were not subject to an information security assessment before an agreement was made, an assessment process should be carried out in order to identify any necessary improvements.

4.3. MONITORING AND REVIEWING SUPPLIER SERVICES

Suppliers will be categorized based on an assessment of their value to the organization, allowing resources to focus on the areas of greatest need.

The performance of strategic suppliers will be monitored regularly according to a combination of reports produced by the supplier in relation to the agreement and analyses produced internally.

Whenever possible, a frequent cross-check will be made between the supplier's reports and those created internally, in order to ensure that the two present a consistent picture of the supplier's performance.

4.4. MANAGING CHANGES IN SUPPLIER SERVICES

4.4.1. Agreement changes

Changes to the services provided by suppliers will be subject to the Forship Group's change management process. This process includes the requirement to evaluate any implications of changes in information security, so that the effectiveness of controls is maintained.

At all times, the degree of risk to the business must be managed and, if possible, minimized.

4.4.2. Agreement termination

The following process will be followed for the scheduled end of the agreement, the early end of the agreement or the transfer of the agreement to another party:

- Termination of the agreement will be requested in writing under the agreed terms.
- The transfer to another party must be planned as a project and the appropriate change control procedures must be followed.
- An assessment of the risk to the organization must be carried out before terminating or transferring the agreement, and contingency plans must be implemented.
- Any budgetary implications must be incorporated into the financial model.

The various aspects of terminating an agreement must be carefully considered when negotiating the initial agreement.

4.5. CLOUD COMPUTING

It is the Forship Group's policy in the area of cloud computing that:

- Data belonging to the Forship Group will only be stored in cloud services with the prior permission of the DTI.
- The appropriate risk assessment should be carried out in relation to the proposed or ongoing use of cloud services, including a full understanding of the information security controls implemented by the CSP.
- Due diligence should be conducted before signing up with a cloud service provider to ensure that the appropriate controls are in place to protect data. Preference will be given to suppliers who are ISO/IEC 27001 certified and who comply with the principles of the ISO/IEC 27017 and ISO/IEC 27018 codes of practice for cloud services.
- Service level agreements and agreements with cloud service providers should be reviewed, understood and accepted before signing up for the service, including GDPR issues.
- Roles and responsibilities for activities such as backups, patches, log management, malware protection and incident management should be agreed and documented before the cloud service starts.
- Procedures must be established to ensure that irreversible activities in the cloud environment (for example, deleting virtual servers, shutting down a cloud service or restoring backups) are subject to adequate controls to prevent errors. Supervision by a suitably qualified second person should be part of such procedures.
- The location of the data stored with the CSP must be understood, and the applicable legal basis must be established, taking into account the country whose law applies to the agreement.
- Multi-factor authentication must be used to access all cloud services.

- The audit log must be available to allow the Forship Group to understand the ways in which this data is being accessed and to identify whether any unauthorized access has occurred.
- Confidential data stored in cloud services must be encrypted using acceptable technologies and techniques. Whenever possible, the encryption keys will be held by the Forship Group and not by the supplier.
- The Forship Group's policies for creating and managing user accounts will apply to cloud services.
- All data stored in the cloud must be backed up. This can be done directly by the Forship Group or under agreement with the cloud service provider.
- All Forship Group data must be removed from the cloud services if the agreement is terminated for any reason.

In general, information security requirements vary according to the type of contractual relationship that exists with each supplier and the goods or services delivered.

5. PENALTIES

Failure to comply with the guidelines of this Policy, even for mere ignorance, will subject the offender to administrative sanctions, including the application of a verbal or written warning, dismissal for cause or agreement termination, as well as subjecting the offender to the other administrative, civil and criminal penalties provided for in Brazilian law.

It is the duty of every employee to notify the Manager of any incident affecting information security, who in turn will refer the matter to the Executive Board for analysis when necessary.