Summary General Information Security Policy

Blumar and Subsidiaries

Policy

The objective of the General Information Security Policy is to set general guidelines for the protection of information assets used at Blumar.

General Objective

Provide continuity for Blumar's operational processes, protecting information assets against internal and external threats that put confidentiality, integrity, and availability at risk.

Information Security

Information security consists of preventive and reactive measures for organizations and technological systems that protect (physical or digital) information from malicious attacks and ensure the confidentiality, integrity, and availability of information.

RESPONSIBILITIES

Responsibility of the employees

All Blumar employees have a responsibility to protect confidential information.

Policy Compliance: All employees must comply with the regulations and procedures established in the information security policy, both at their workplace and outside of business hours. This includes proper use of systems and applications that handle sensitive information.

Incident Alert: If an employee identifies an incident that affects the confidentiality, integrity, and availability of information they must notify their supervisor and/or the Information Security Committee in a timely and appropriate manner.

Information Protection: All employees must protect confidential and sensitive information and prevent unauthorized disclosure to third parties.

Employees must rigorously comply with and accept the information security controls that Blumar performs to ensure compliance. Blumar reserves the right to take disciplinary action against any employee who does not comply with the Information Security Policy.

Responsibility of the suppliers

Suppliers providing services to Blumar must comply with information security requirements set forth by Blumar to protect sensitive and confidential data.

Service Levels: Providers must comply with the service levels established by Blumar to ensure the availability and accessibility of services. These service levels should be defined in the contract with the supplier and should be reviewed and updated periodically.

Business Continuity: Providers must have mechanisms in place to ensure the availability of their services in the event of an outage. These mechanisms should include backup and recovery plans for emergency situations to ensure the integrity and availability of information.

Confidentiality and Non-Disclosure: Suppliers must comply with the conditions set out in the contract, even after the termination of the service contract. This includes an obligation to protect and not disclose confidential information to third parties.

Emergency Alert: Providers must notify Blumar immediately in the event of an information security emergency. This notification should include a detailed report on the emergency and the measures taken to resolve it.