

SUPPLIER SECURITY REQUIREMENTS

Introduction

fabbricadigitale recognizes supply chain security as a fundamental element in protecting information, information systems, and the digital services it delivers.

This document outlines the principles and minimum security requirements that may be applied to suppliers and business partners who, directly or indirectly, contribute to the delivery of our products and services.

General Principles

Suppliers are expected to implement organizational and technical security measures that are appropriate to the level of risk associated with the services they provide.

The measures adopted should contribute to ensuring:

- Confidentiality of information;
- Integrity of data;
- Availability of services;
- Business continuity;
- Traceability of relevant activities.

Security Management

Suppliers are expected to maintain security controls that are appropriate to the nature of the services provided and the associated level of risk.

fabbricadigitale may request supporting documentation, including but not limited to Information security certifications, Statements of compliance, Security questionnaires or equivalent documentation.

Incident Management

Suppliers are required to notify fabbricadigitale without undue delay of any security incident that may affect the services provided, the information processed, the confidentiality, integrity, or availability of systems or data, business continuity.

Notifications should include sufficient information to enable an appropriate assessment of the incident, its potential impact, and any mitigation measures already implemented or planned.

Business Continuity

For services considered critical, suppliers are expected to implement appropriate business continuity and disaster recovery measures to ensure service resilience and timely restoration in the event of disruptive incidents.

Periodic Review

fabbricadigitale may periodically assess suppliers whose services are considered relevant from an information security perspective in order to verify the continued fulfilment of the applicable security requirements.

Disclosure Policy

Security is an ongoing process that benefits from collaboration between organizations, customers, users, and the security research community.

fabbricadigitale encourages the responsible disclosure of security vulnerabilities affecting its systems, applications, or digital services.

Security vulnerabilities can be reported by email to: servicedesk@fabbricadigitale.it

Upon receiving a vulnerability report, fabbricadigitale is committed to:

- acknowledging and reviewing the report;
- assessing the information provided;

- determining and implementing appropriate corrective actions where necessary;
- maintaining constructive communication with the reporting party throughout the assessment process.

Information received through the Responsible Disclosure process contributes to the continuous improvement of fabbricadigitale's information security practices and helps strengthen the resilience of its digital services.