EMEIA Security Master Policy

Master Policy Statement

Fujitsu EMEIA operates in a business environment which requires that:

- As individuals, we adopt a culture that minimizes the security risks to our people, assets and business activities;
- As an organization we have an effective security management and governance framework that allows Fujitsu EMEIA to take informed business decisions to successfully manage security risk.

This Master Policy is the foundation of Fujitsu EMEIA's Information Security Management System and an integral part of the EMEIA Business Management System. The objective is to deliver an effective and managed approach to security across our business.
Fujitsu EMEIA has developed the Security Policy Manual as a single set of mandatory principles in support of this Policy.
This Policy and the Security Policy Manual detail the minimum required by all Fujitsu EMEIA employees. Additional local policies and customer requirements may be more stringent than this and should be followed where applicable. Where a customer contract requires a lower level of security this must be captured as a risk in the Risk Plan and formally authorized by an exemption obtained through the EBMS Process Exemption Procedure.

Authority & Accountability

The EVP Head of EMEIA has ultimate responsibility for security.

The EMEIA Corporate Governance Committee (CGC) delegates its security governance responsibilities to the Risk and Governance Management Board (RGMB) and through the RGMB to the Security Management Board, and the Security Governance function.

The RGMB is responsible for ensuring that Fujitsu EMEIA has an effective approach to risk management. For security risks, the RGMB is responsible for ensuring that an effective security risk management approach is adopted in all the operating areas of Fujitsu EMEIA (divisions, business functions and business lines). This approach must embed responsibility and accountability within the operational structure of Fujitsu EMEIA.

Fujitsu EMEIA will seek to ensure that its working partners and any joint ventures or consortia, in which it is engaged, have the required Management Systems in place to achieve adequate standards of information security performance consistent with the expectations of Fujitsu EMEIA, as described in the Security Policy Manual.

The Policy Owner shall:

a) Ensure that all relevant Employees are aware of and, where appropriate, trained in the operation of this Policy and any changes to it;

b) Ensure that any changes to the Policy or its associated Processes are duly authorized by the Security Management Board;

c) Submit a regular report on the effectiveness of this Policy to the EMEIA Corporate Governance Committee;

d) Ensure that Processes are specified and maintained to enable Fujitsu EMEIA to achieve its strategic objectives in respect of this Policy.

Employees

Each Employee in the organizations to which this Policy is applicable (see below – Applicability) must comply with this Policy, the Security Policy Manual, and associated Processes, security controls, standards and guidelines, which are published in the EBMS.

Any Employee found to be in breach of any Policy, or any employee who neglects personal security responsibilities as laid down in the Global Business Standards, may be subject to disciplinary proceedings that may lead to dismissal.

Applicability

This Policy applies to Fujitsu operations in EMEIA. This means that all Employees, Contractors, Working Partners and businesses carried on by Fujitsu Services Holdings PLC, Fujitsu Technology Solutions (Holding) BV and their subsidiaries, whether they be incorporated within Fujitsu EMEIA or not, and any other company or organization that is managed by the Head of EMEIA Region, except to the extent, if any, stated under Exemptions below, must comply with it.

Exemptions

None.

For Further Information:

securitygovernance@uk.fujitsu.com