Overview of G4S Netherlands information security policy

Purpose and scope of the document

The purpose of this document is to give customers, vendors or other parties an overview of the information security policy of G4S Netherlands.
Information in this document is only provided to give a high level overview and this document cannot be seen as the formal information security policy of G4S. No rights whatsoever can be derived from using this document.

G4S Group Information Security Policy

G4S Netherlands is part of the larger G4S international organisation. G4S Group has several policies, including information security policy, that are applicable to all countries. Each country organisation has the obligation to comply to the group policies.

Structure

The G4S information security policy is part of a wider cyber security framework. This includes G4S Group Best Practice Guidance and Instructions, specific security enforcing controls, regional and local risk management decisions and information security procedures. G4S has adopted the international information security standard ISO 27000 series as its model for information security.
The G4S information security policy has consolidated and incorporated G4S regional and business policies, giving room to regional or country market needs, specific rules and regulations.

Security Controls

The Mandatory Minimum Security Controls (MMSC) is the set of information security controls that must be applied to all G4S businesses; it is the implementation of global policy. G4S uses compliance against the MMSC to ensure that information assets are appropriately protected.
The mandatory control set has been approved by the Group Information Security Committee

The MMSC includes the following controls: Mandatory adoption of the Group policy, Coordination of information security activities, Risk assessment, Acceptable Use Policy, Disposal of IT assets, User lifecycle processes, Password policy, Physical protection servers and end point computing, Change control, Security testing, Secure software development lifecycle, Incident management, Backup policy, and Network policy.

ITIL

G4S Netherlands has adopted ITIL for its incident, problem and change processes. A global service platform has been implemented where incident, problems and changes are registered, handled and monitored.

Outsourced IT infrastructure

G4S Netherlands has outsourced the majority of its IT infrastructure to KPN, a large telecom and IT service provider in the Netherlands. G4S Netherlands runs its primary systems in a dual data center, as part of KPN's IT services provided to G4S.
KPN has the following certifications for its datacenter and workplace online services: Information security 27001:2005, Business continuity BS 25999:2007, Servicemanagement ISO 20000, and ISAE-3402 declaration.

GDPR / Data protection officer

G4S appointed several data protection officers through Europe. These officers are responsible for implementing and monitoring the General Data Protection Regulation (GDPR). In case of the Netherlands, incidents can be reported by calling +31 (0)20- 51 48 888. Further question can be sent to privacy@nl.g4s.com.