Generic Information Security Requirements LVNL

Reference	
Version number	1.1
Version date	March 2020

Status	Concept
Classification	LVNL Internal

1. Introduction

Air Traffic Control the Netherlands (LVNL) is delivering Air Traffic Control (ATC) services to users in the Dutch national airspace. At LVNL, Information Security is part of ATM security, next to Physical Security and Personnel Security. LVNL's Information Security Management System (ISMS) is based on ISO 27001 (Plan-Do-Check-Act) and ISO27002 (Best Practise implementation). International legislation and guidance is taken into account, like Regulation (EU) No. 1035/2011 (Common Requirements), Regulation (EG) No. 482/2008 (ESARR 6), ICAO Doc. 9985 and ICAO Doc. 8973 and EN 16495:2014 (Information security for organisations supporting civil aviation operations). Furthermore, Dutch legislation (on privacy, data classification, etc.) is applicable to LVNL.

LVNL has been identified as a critical stakeholder in a vital process to the Netherlands' economy: *a swift and secure flight- and aircraft handling*. Therefore, the focus of Information Security at LVNL is on availability (continuity).

This document describes generic Information Security Requirements of LVNL that vendors should fulfil in order to qualify for doing business with LVNL.

2. Generic Information Security Requirements

Information Security Management System
- The tenderer must have an Information Security Management System (ISMS) in place describing a Plan-Do-Check-Act cycle on the implementation of information security (for example ISO27001).
- The ISMS must be audited on a regular basis by an external, independent auditor. Audit reports must be provided to LVNL on request.

Cyber resilience
- The tenderer must have measures implemented to prevent, detect and mitigate attacks on its own (development) systems and infrastructure. In case of an attack and/or breach the vendor has to inform LVNL immediately.
- The security measures must meet the level of protection provided by the current technological state of the art.

Physical security
- The tenderer must have physical measures in place to prevent unauthorized access to the premises and locations related to the services or products of the tender.

Personnel security
- The tenderer must have a process in place to guarantee that the employees involved in or working on the services or products of the tender have the appropriate qualifications.
- The tenderer must have a process in place to guarantee the that the employees involved in or working on the services or products of the tender have undergone an appropriate security screening.

Personal Data
- LVNL and the tenderer must comply to GDPR on the protection of personal data. Before personal data is stored at or transferred to data processors outside the EU, a data processing agreement based on the EU model clauses must be signed.

Compliance monitoring
- LVNL has the right to have security audits and/or penetration tests performed by an auditor, chosen by LVNL, where the scope of the audit / test are the services or products of the tender. Audits / tests will always be performed in alignment with and in agreement with the tenderer.
- In case of vulnerabilities found in audits / tests, a corrective measure will have to be presented to LVNL within 10 working days. The corrective measure will be solved at the cost of the tenderer.
- All of the above must be formalized and maintained in security documentation by the tenderer.

3. Contact information

The tenderer must assign a security officer who will act as a single point of contact for LVNL. LVNL's security officer can be reached through security@lvnl.nl .

Luchtverkeersleiding Nederland / Air Traffic Control the Netherlands

Stationsplein Zuid-West 1001
1117 CV Schiphol

Postbus 75200
1117 ZT Schiphol

T 020 406 2000

www.lvnl.nl