Technical & organisational security measures

This is an English translation of the Swedish original – in case of discrepancies between the documents the Swedish version shall prevail.

1 General

1.1. Hogia ensures that any delivery provided by Hogia has adequate security protection measures in place, to meet the provisions set out in this document and in the relevant agreement.

1.2. Hogia strive to abide and adhere to MSB's (Swedish Civil Contingencies Agency) framework to establish and employ an Information Security Management System (LIS) based on international standards in the ISO 27000 series. Hogia have an information security policy in place that demonstrates Hogia's adherence.

1.3. All Hogia employees are covered by confidentiality agreements.

1.4. Hogia's undertakings regarding security protection measures include, but are not limited to, the following:

a) Hogia ensures that security systems and administration tools are used only as intended.
b) Hogia ensures that security awareness training and information has been given to all personnel of Hogia involved in Hogia's deliveries.

1.5. Security incident management. In case of a security incident affecting a Customer, or with the potential to affect a Customer, Hogia will - without undue delay - report to the Customer contact person.

1.6. Within the Hogia organization, there is a position Head of Security responsible for security matter communication

- Chief Security Officer (CSO) securitygroup@hogia.se
- Chief Information Security Officer (CISO) ciso@hogia.se
- Chief Privacy Officer (CPO) gdpr@hogia.se

1.7. A documented and implemented continuity- and crisis plan which is regularly revised and practiced is in place at Hogia. The planning includes different forms of risk management.

2 Baseline security

This section covers Hogia's continuous baseline security operations.

2.1 Hogia IT environment

2.1.1 Asset management
Assets associated with information and information processing are defined, registered, and updated in a central register maintained by Hogia.

2.1.2 Change management

Changes to infrastructure, servers and hosted systems and services are performed and approved in accordance with the Hogia Change Management Process. The change procedures ensure control over all security related changes.

2.1.3 Backup

Backup is performed regularly and stored in a geographically different location from the operating environment.

2.1.4 Protection against malicious software

Controls for prevention from and detection of malicious software are continuously carried out to ensure the capacity to - at best effort - detect, remove, and protect against, malicious software in Hogia's IT environment.

2.1.5 Technical vulnerabilities in systems and services are continuously monitored and managed.

2.1.6 Systematic penetration tests are constantly performed on systems and services, either exposed to the Internet or internally within Hogia. Customers may not perform their own penetration tests on their systems run at Hogia without Hogia's previous written acceptance hereof.

2.1.7 Security protection of systems and services in network.
Only approved assets may connect to Hogia's network. Authorisation is required to obtain access to systems and services connected to the Hogia network.

2.1.8 Hogia applies secure processes in the development of software and services.

2.1.9 With regards to our systems, services, processes etc., Hogia is continuously working on data protection matters (e.g. GDPR compliance).

2.1.10 Access control
Access control routines applies for all access to Hogia's networks, systems, and services regardless of whether access is initiated by the Customer, by Hogia or by a Hogia subcontractor. Access control includes, but is not limited to:

a) Administrative accounts, used by Hogia for Hogia systems and services, are defined, documented, and maintained only by employees for whom access is required to carry out their missions (based on need-to-know and least privilege principles).
b) Administrative accounts and access rights are assigned to a user account different from the accounts used for daily operations.
c) Individual user identities are required regardless of whether these are used for daily operations or for administrative purposes.
d) Administrative access rights are reviewed and documented on a quarterly basis.
e) Requests for new administrative accounts and access rights to systems and services are formally documented and approved by the appropriate organisation.
f) All access rights for a leaver are deactivated upon termination of employment.
g) The use of high-quality passwords (e.g. requirements on length and complexity) is maintained.
h) Passwords are securely stored and transmitted to avoid being compromised.

2.2 Installation and start-up – Customer's IT environment

2.2.1 Access control

a) Default and temporary passwords and cryptographic keys in the systems and services are changed into unique values prior to use.
b) All Hogia access rights shall be deactivated or deleted before hand-over to Customer.
c) Information regarding how high-quality passwords, through length and complexity, is maintained shall be given to the Customer.

2.2.2 Hogia will not change security solutions ordered and implemented by a Customer without first obtaining the Customer's written approval.

3 Other security

3.1 Remote support

3.1.1 The Customer's chosen method of remote access to the Customer's data will be observed by Hogia. As part of the access granted to Hogia by the Customer or by a Customer representative, Hogia may take part of all data including personal data and information generated during the remote support session. If no such method exists, Hogia will recommend a method based on secure communication and multi factor authentication.

3.1.2 Customer data handling
Information sent to Hogia for troubleshooting, or for other reasons, will be classified and handled as confidential information.

3.2 Physical security – Hogia data centre

3.2.1 Secure areas are protected by appropriate entry controls to ensure access that only authorised personnel are allowed access.

3.2.2 The cooling, power and communications infrastructure of our data centre is redundant. The primary data centre is classified as a high security data room of protection class R60 as per EN 1047-2:2009 + A1:2013 and ECB-S C10.

3.2.3 Access lists to secure areas are reviewed and documented every six months.

3.2.4 Requests for access to secure areas are formally documented and approved by the appropriate organisation.

3.2.5 Physical protection against natural disasters, malicious attacks and accidents has been developed and is in use.

3.2.6 Data carrying power and communication cables are protected from interception, interference, and damage.

3.2.7 Equipment is correctly maintained to ensure its continuous availability and integrity.

3.2.8 The protection of equipment in other locations is based on the risk assessment of managing this equipment outside the Hogia facilities.