Vendor Information Security Instruction

Dok. nr. OKEA-SEC-WIN-0207

Dokument nr.	OKEA-SEC-WIN-0207
Revisjon nr.:	3.0
Dato:	24.10.2022
Erstatter dok.nr.	
Prosjekt:	Information Security
Disiplintype:	Security
Dokumenttype:	Instruction
Opphavsperson:	Information Security Officer
QC (Sjekket):	Manager IT & Digital Transformation
Godkjent:	SVP Business Performance

1 Background

OKEA´s information assets are managed with the support from trusted vendors with access to OKEA´s information and information systems. OKEA´s effective security level comprises the combined performance of OKEA´s processes and employees, and those of our affiliates.
Any access can be exploited for harmful intentions, directly or indirectly, and use can have unintentionally negative consequences.

2 Purpose

To reduce the risk of any information security breaches through vendors deliveries, this document outlines OKEA´s requirements and expectations for vendors information security performance.

3 Requirements

All vendors with access to OKEA´s information systems shall:

- adhere to OKEA's security practices, incl. the 'Procedure for Acceptable Use of IT systems' (OKEA-SEC-PRO-185), and communicate any situations where this adherence is not achievable, helping to prevent security gaps or conflicts that could impair security performance,
- have processes in place to inform personnel with access to OKEA's information systems about relevant requirements,
- provide a designated focal point to respond to any enquiries from OKEA regarding the vendors personnel, tasks, access level and justification for access in a timely matter,
- have a process to periodically review and assess their personnel's access to OKEA´s information systems,
- participate in OKEA´s Information Security awareness program as required by OKEA contract owner or Information Security Officer,
- ensure that OKEA systems and information is only accessed and handled digitally through the use of safe and appropriate end-user equipment. Such equipment includes contractors' personal laptops and smartphones, risk-assessed by the issuing organization,
- inform OKEA in a timely manner regarding changes that may impact OKEA's business, and
- have a process to notify OKEA Service Desk without delay of;
    - any changes in need for access,
    - relevant incidents, suspicions or vulnerabilities affecting systems or equipment used to access, store or process OKEA´s information. Examples includes;
        - loss or theft of personal equipment or other information systems (note that mobile phones are often used for secondary authentication codes),
        - theft of or unauthorized disclosure of authentication details to information systems, incl. personal equipment used to access OKEA systems,
        - compromised information systems, such as any malware infections including spyware and crypto-viruses or hacked accounts, and
        - shared accounts and weak authentication mechanisms, incl. system integrations.

Information systems include personal computers, mobile phones, networks, storage and processing systems, cloud services, e-mail systems, internet browsers, etc.

4 Controls

As a measure to ensure compliance with established principles, OKEA reserves the right to review vendors practice of and adherence to Information Security principles. Vendors may also be expected to provide independent evidence that its IT security provisions comply with contractual requirements. This can be achieved, for example, by a third-party audit with scope and cost agreed upon by the vendor and OKEA.