Sval

Cyber Security Instructions to Vendor

All vendors with access to Sval Energi´s information systems shall:

- adhere to Sval Energi's security practices, incl. the Acceptable Use Standard, 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 Sval Energi information systems about relevant requirements,
- provide a designated focal point to respond to any enquiries from Sval Energi 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 Sval energi's information systems,
- participate in Sval Energi's Information Security awareness program as required by Sval Energi contract owner or ICT Security lead,
- ensure that Sval Energi systems and information is only accessed and handled digitally through the use of safe and appropriate end-user equipment. Such equipment includes vendors' personal laptops and smartphones, risk-assessed by the issuing organization,
- inform Sval Energi in a timely manner regarding changes that may impact Sval Energi business,
- have a process to notify Sval Energi 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 Sval Energi's information. Example incidents or suspicion of such includes;
    - loss or theft of personal equipment or other information systems. Note that mobile phones are often used for secondary authentication codes (2FA/MFA),
    - theft of or unauthorized disclosure of authentication details to information systems, incl. personal equipment used to access Sval Energi systems, and
    - compromised information systems, such as any malware infections including spyware and crypto-viruses or hacked accounts.
    - 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.

As a measure to ensure compliance with established principles, Sval Energi 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 Sval Energi.