Cyber Security Standards for Suppliers

Section A - all suppliers

ALL suppliers are expected to meet the Cyber Security Standards detailed below.

1. Suppliers must be able to demonstrate a culture of cyber security awareness within their organisation. This includes, but is not limited to:
    I. evidence of any registration against a recognised Cyber Security Standard (e.g. those detailed in Cyber Essentials);
    II. cyber security training of employees, including an ongoing programme of improvement;
    III. robust backups; incident response policies; and disaster recovery plans etc.

2. Phishing and malware can often originate from compromised suppliers. Therefore, suppliers must demonstrate robust cyber security systems. This includes:
    I. email systems using Multi-Factor Authentication or other protective measures, e.g. DMARC;
    II. processes in place to ensure active notification at the earliest opportunity if the supplier detects that its systems have been compromised or involved in Phishing.

3. In the event of Phishing or malware compromise, which originated from the supplier and was detected by INEOS Inovyn, there must be a clear escalation route to the supplier.

4. Financial fraud is often attempted by intercepted emails that request the receiver to change their bank details. As part of the INEOS Inovyn Anti-Fraud Policy, suppliers need to have a clearly stated process by which they would notify INEOS Inovyn of legitimate changes, with named contacts for INEOS Inovyn to use for independent checks to confirm validity.

5. Suppliers storing data related to INEOS Inovyn must ensure that such storage conforms to the Legal Data Protection requirements depending on each country, including:
    I. General Data Protection Regulation (GDPR) compliance or equivalent;
    II. INEOS Inovyn data stored on portable devices, e.g. laptops, should use full disk encryption.

6. Any method used for transferring software or data as part of the supplier's work must use suitably secure mechanisms, such as:
    I. an INEOS Inovyn hosted SharePoint secure site;
    II. a secure file transfer site provided by the supplier that has been certified by INEOS Inovyn.

7. Mass transfer devices such as USB sticks/drives are to be used only when no other practical mechanism exists and must in all such cases conform to INEOS Inovyn policies and checks at the time of use.

INEOS Inovyn

Section B - suppliers of systems and resources to work on INEOS Inovyn systems

In addition to Section A, ALL suppliers of systems, equipment and resources who will work on INEOS Inovyn systems must ensure that the following additional requirements are met.

8. Supplied systems and any re-badged equipment must use vendor- supported platforms with a minimum expected lifetime of 5 years. This includes aspects such as:
    I. Operating Systems (OS);
    II. firmware;
    III. reliance on any third-party applications, components and web browsers.

9. Supplied systems must be capable of being **updated against future vulnerabilities**, for example:
    I. application of regular operating system patches;
    II. application of operating system version updates;
    III. the supplier must state its process for testing and approving patches, e.g. duration of supplier approval phase, special arrangements for particularly critical patches.

10. Supplied systems must have the capacity for cyber protection, including measures such as:
    I. basic anti-virus protection;
    II. protection by application whitelisting;
    III. advanced malware protection;
    IV. network protection by firewall devices;
    V. the supplier must not be identified by the government as inherently cyber insecure, and therefore subject to restrictions.

11. If a supplier is granted remote access to INEOS Inovyn systems, any such access must only be used for the intended purpose, and only to the systems identified in the scope of the support, service-level agreement (SLA), etc:
    I. all such work must be agreed with INEOS Inovyn before taking place and be subject to regular review (per annum at minimum).

12. In the case of granted remote access to any part of INEOS Inovyn systems, additional requirements may be required, such as:
    I. named individuals only - including possible background checks, proof of training, agreed named deputies etc.;
    II. second-factor authentication to be held by INEOS Inovyn.

13. Where suppliers are providing resource rather than systems to INEOS Inovyn, it is expected that all resources will work within the INEOS Inovyn guidelines for cyber security, both while on our sites or elsewhere while engaged in INEOS Inovyn-related work. Such guidelines would normally be communicated as part of the INEOS Inovyn induction process.

END OF DOCUMENT

V1. August 2020