Technical Vulnerability Management Policy

Contents

Background 2
Scope 2
Accountabilities 3
Policy Statements 3
Policy Compliance 4

Distribution List

☐	CEO	☐	COO
☐	CFO	☐	Country Managers
☐	Internal Only	☐	Internal and External
☐	All Staff	☐	Board Members

Revision History

Created: 23rd September 2020
Updated: 21st January 2022

Background

Technical Vulnerability Management is the ongoing, risk-informed process of addressing weaknesses on Information Technology (IT) infrastructure, operating systems, and applications. If left untreated, it could allow malicious exploitation leading to the compromise of Departmental assets. The weakness could be addressed with application of a patch or a change in the configuration of the system.

CompanyX applies a risk-focused approach to technical vulnerabilities. It is accepted that systems and services must have a proportionate and appropriate level of security management.

As a result, this policy adopts an exception-based risk management approach – compliance is mandated unless an exception is granted (see the Policy Compliance section below).

This policy requires all Digital Product Owners to be accountable and responsible for establishing a programme for the identification and remediation of technical vulnerabilities across:

a) IT infrastructure, including hardware, firmware, middleware, and network devices
b) operating systems
c) applications; and
d) network appliances (anything connected to the corporate network not included above)

This policy sets out the requirement to identify and address technical vulnerabilities quickly and effectively, reducing the likelihood of them being exploited, which could result in serious security breaches and damage to companies' reputation.

Scope

The scope of this policy is to define the Department's requirement for:

a) finding known and discovering new technical vulnerabilities, across all environments (i.e., Production, Pre-Production, Test and Development)
b) scanning for known and new technical vulnerabilities using IT Health Checks (ITHCs), Penetration Tests (including Red Teaming), and Continuous Vulnerability Monitoring both to discover new weaknesses and to confirm that patches/configuration changes have been applied correctly
c) managing technical vulnerabilities (e.g., using a patch management process, automated remediation tool, and / or a configuration change).

This policy does not replace any legal or regulatory requirements.

This policy applies to all contractual agreements for the provision of computing and networking services for the Department and these policy statements supplement all currently applicable contractual agreements to Departmental computing and networking services.

This policy applies to:

a) *CompanyX* assigned staff designing, implementing, and running new and current IT solutions
b) any suppliers, whose systems or services store, handle, or process information; to ensure the appropriate levels of assurance for the confidentiality, integrity, and availability of the Department's assets

Accountabilities

The Chief Technology Officer is the accountable owner of the Technical Vulnerability Management Policy and is responsible for its maintenance and review.

Accountability and responsibility for the security for each system / service must be appropriately agreed and allocated between IT and the Chief Operating Officer.

Policy Statements

Accountable parties are required to ensure people and processes are in place to perform the activities required for technical vulnerability management as outlined in this policy. Accountable and responsible parties are required to have in place processes to monitor progress on technical vulnerability management so that they are satisfied that the requirements of the policy are being fulfilled.

All responsible parties are required to develop and maintain processes which ensure that the following responsibilities are managed in a timely fashion:

a) technical vulnerability identification
b) technical vulnerability analysis; and
c) delivery of remediation to assets (e.g., through patching or reconfiguration), including the testing of the remediation.

Security testing and technical vulnerability scanning of *CompanyX* business applications, operating systems, and network devices, including all *CompanyX* supplier systems and services which store, handle, or process *CompanyX* information must:

a) identify new technical vulnerabilities
b) check if security measures have been applied correctly and successfully
c) assist in the prioritisation of the remediation of vulnerabilities
d) provide a view of vulnerabilities across the organisation's technical infrastructure (e.g., to make comparisons and identify trends).

Security testing and technical vulnerability scanning of business applications, operating systems and network devices must be:

a) performed on a regular basis informed by the risk function
b) proportionate; and
c) in compliance with this policy.

Security testing and technical vulnerability scanning must be proportionate to the value of the asset as defined by the security risk function. Security testing and technical vulnerability scanning is likely to include:

a) automated technical vulnerability scanning software or a commercial vulnerability scanning service; and / or
b) penetration testing and / or Red Team Exercises.

Where remediation can be undertaken that is straightforward and with a low risk of impacting availability, confidentiality, or integrity, then it must be carried out as a matter of course.

a) The process for remediating technical vulnerabilities must be developed and undertaken following consultation between IT and any impacted busines service owners including HR.

b) an assessment of the risk, and a documented decision-making process on how the risk will be managed, including regularity and frequency of remedial actions. This process must include steps where appropriate for escalating if the risk posed is above the Department's agreed tolerance
c) a way of recording patches that have been applied (e.g., in a specialised patch management tool or a Configuration Management Database (CMDB)
d) testing patches prior to deployment, or applying for and receiving an exception to the policy
e) deploying patches to systems that are not accessible via the corporate network (e.g., standalone computers) or devices that connect to the corporate network infrequently (e.g., mobile / home workers)
f) dealing with the failed deployment of a patch (e.g., redeployment of the patch)
g) reporting on the status of patch deployment
h) protecting information when a technical vulnerability cannot be remediated with a patch, or an available patch cannot be applied (e.g., by disabling services, adding additional access controls, and performing detailed monitoring).

Security testing and technical vulnerability scanning must be undertaken with the prior agreement of the Product Owner

The only admissible exceptions to this consent are:

a) a security test or technical vulnerability scan required by IT
b) a security test or technical vulnerability scan required to assist with the resolution of a live incident
c) undertaken by a limited number of authorised individuals (e.g., using a dedicated account that is only used for technical vulnerability scanning)
d) performed using approved and dedicated systems
e) independently monitored (e.g., to identify misuse by authorised individuals or help detect unauthorised scanning).

Policy Compliance

Where technical remediation (e.g., patches) is not applied in line with this policy, an exception to the policy must be sought from the *CompanyX* risk management function.

If the potential consequence of patching-levels of a system exceeds the risk tolerance a report must be made to the *CompanyX* risk management function which will agree and oversee, with the Accountable Owner(s), a plan to manage the system / service risks.

Compliance to this policy will be declared through annual attestation to the policy. Accountable parties must be prepared and able to evidence compliance to this policy, if appropriate with technical vulnerability output from their compliant network.