Windows Server Security Checklist

System Installation & Patching

1. If machine is a new install, protect it from hostile network traffic until the operating system is installed and hardened. ☐

---

2. Only use Supported Windows Operating systems and applications. ☐

(Microsoft no longer supports XP and Windows 2003 server).
Visit - https://support.microsoft.com/en-us/lifecycle?C2=1163

3. Set Windows systems Patches to automatically install. ☐

Make sure users log out of the server each evening so that Windows patches can be applied.

4. Enable system and event logging. ☐

OS Hardening

1. Make sure that all application patches are kept up to date. ☐

E.g **Java, Sql_server, Oracle, adobe,** etc

2. Install **Microsoft Enhanced Mitigation Experience Toolkit "EMET"** to defend against cyberattacks. ☐

Visit - https://www.microsoft.com/en-us/download/details.aspx?id=50766 - EMET will reach end of life on July 31, 2018. The successors to EMET are the *ProcessMitigations Module* - aka *Process Mitigation Management Tool* - and the *Windows Defender Exploit Guard* only available on Windows 10 and Windows Server 2016.

3. Install **Anti-Virus.** ☐

Remember to check it at least once a week to ensure that it is running, update and review the last full AV scan results. If using **Sophos** manually enable **"Web Protection"**.

4. Run **Microsoft baseline security analyser** to check security setting. ☐

Visit - https://msdn.microsoft.com/en-us/library/ff647642.aspx

5. Microsoft recommend disabling **SMB1** due to its high vulnerability to malicious software. ☐

Further information and steps to disable SMB1 are listed below.
Visit - https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/
Software packages that still require SMB1 be enabled are listed below:
Visit - https://blogs.technet.microsoft.com/filecab/2017/06/01/smb1-product-clearinghouse/

6. Remove or disable all Internet browsers **(Windows feature > disable IE)**. ☐

If a browser is absolutely required enable IE with enhanced security configuration.
Running the following **PowerShell** command as administrator will also disable Internet Explorer **dism /online /disable-feature /featurename:Internet-Explorer-Optional-amd64**

User Access & Passwords

1. Create an account for each user who should access the system. ☐

Avoiding shared accounts/passwords makes it easier to keep an audit trail and remove access when no longer needed.

2. Enforce the use of strong passwords. ☐

Run **"Secpol.msc"** and edit **"Account Policies"** - Create a strong password policy by setting a minimum password length of 10 and enable password complexity requirements.

3. Configure an intrusion prevention policy. ☐

Run **"Secpol.msc"** and edit **"Account lockout policy"**. - Set accounts to lockout for period of time **(min 10 minutes)** after a small number of failed login attempts **(5)** and reset account lockout counter to the same period as lockout (e.g 10 minutes)

4. Enable user account control (UAC) ☐

So that system changes require administrator level permissions.

5. Create an account for each user who should access the system. ☐

Avoiding shared accounts/passwords makes it easier to keep an audit trail and remove access when no longer needed.

6. Check that only approved users can access the server and that they only have the minimum privileges necessary. ☐

Do not use generic accounts and remove unnecessary accounts such as guest.

Network Security & Remote Access

1. Use the local firewall to restrict **Remote Desktop Access** to only the UCD network (or preferably your own network) and use the **UCD VPN** if remote access is required. ☐

The VPN range details are:
Staff Profile: 137.43.50.0/24
Research Profile: 193.1.162.0/24

2. To protect against phishing (and malware) attacks never access email on server and remove all email clients. ☐

---

3. Use **SSL** for all websites. ☐

This is a requirement for any website that requires authentication. Detailed instructions on how to obtain a **free SSL certificate** can be found here.

4. Disable or uninstall all unnecessary Windows services and features. ☐

---

e.g **print service**, **file and printer sharing**, **netbios**, etc

5. Check that the server Firewall is turned on and filterers are setup to protect open ports and programs. ☐

Registered UCD servers are accessible across the entire UCD Network and a number of common ports are open to the internet which may include **22**, **53**, **80** and **443**. Please ask security@ucd.ie if these ports are open in your network.

However all ***TPC & UDP ports over 1024*** are internet accessible on all registered servers regardless of the network, so this means that default ports such as **SQL_SERVER (1433)**, **Remote Desktop (3389)**, **Oracle listeners (1521)**, etc. can be accessed from outside of UCD putting your information at risk if not protected by the local firewall. Use of non-standard ports for **RDP** traffic instead of the default **3389 TCP/UDP** is advised.

Do not collect or process credit card payments on any server without contacting security@ucd.ie in advance.

Once you have applied the above hardening recommendations then contact Security@ucd.ie for free vulnerability scan.

Security Tip: Protect your information visit www.ucd.ie/itsecurity