Windows Server Security Checklist

	Recommendations	**Completed**	**Comment**
1.	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		
2.	Set Windows systems Patches to automatically install. Make sure users log out of the server each evening so that Windows patches can be applied.		
3.	Make sure that all application patches are kept up to date. E.g Java, Sql_server, Oracle, adobe, etc		
4.	Install Microsoft Enhanced Mitigation Experience Toolkit "EMET" to defend against cyberattacks. Visit - https://www.microsoft.com/en-us/download/details.aspx?id=50766		
5.	Create a strong password policy. Run "Secpol.msc" and edit "Account Policies" - Set a minimum password length of 10 and enable password complexity requirements		
6.	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)		
7.	Install Anti-Virus and remember to check it at least once a week to ensure that it is running, updating and review the last full AV scan results. If using Sophos manually enable "Web Protection".		
8.	Enable system and event logging.		
9.	Check that the server Firewall is turned on and filterers are setup to protect open ports and programs.		
10.	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.		

11.	Disable or uninstall all unnecessary Windows services and features e.g print service, file and printer sharing, netbios, etc		
12.	Remove or disable all Internet browsers (Windows feature > disable IE) or if absolutely required enable IE with enhanced security configuration.		
13.	To protect against phishing (and malware) attacks never access email on server and remove all email clients.		
14.	Enable user account control (UAC) so that system changes require administrator level permissions.		
15.	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.		
16.	Use SSL for all websites. This is a requirement for any website that requires authentication. Contact security@ucd.ie for free SSL certificates.		
17.	Do not collect or process credit card payments on any server without contacting security@ucd.ie in advance.		
18.	Run Microsoft baseline security analyser to check security setting.		
19.	Once you have applied the above hardening recommendations then contact Security@ucd.ie for free vulnerability scan.		