Network Change Request

Return completed form to Security@ucd.ie. Changes are reviewed within one working day. Implementation for requests up to Monday 11am is the following Tuesday.

Please complete ALL sections (A- G)

Section A: Requester Details	
Name:	
Personnel Number:	
Email:	
Telephone:	

Section B: Project\System	
Name of Server:	
IP Address of system:	
Registered UCD System Owner:	
Description of services hosted on server:	
Does the server contain any confidential data? **If Yes please describe type of data:** **Please check Data Classification Guide**	

Section C: Overview and Description of Request					
Description of change required	**Details:**				
	Allow From: Server / IP Address: (Example: Allow from outside of UCD)	**Allow To: Server / IP Address** (Example: MyServer.ucd.ie / I37.1.1.2.3)	**Port & Protocol**	**Allow\Deny**	

Section F: Impacted Users & Potential Risks

Section E: Security Requirements

The following are the recommended server hardening standards for UCD servers.

Linux

- Apply latest patches and configure automatic security updates
- Install Sophos Anti Virus for Linux free from Sophos.com
- Disable root login (use sudo)
- Use strong passwords (Minimum 10 characters using a combination of mixed case letters, numbers and symbols. The higher number of characters the stronger the password)
- Configure I.P tables for all open ports.
- Use SSL for all websites. – IT Services offer free SSL certificates.
- Configure free Fail2ban software to prevent brute force attacks.
- Remove unnecessary services and protocols (Telnet, IPv6, KDE/GNOME, etc)
- Ensure you have adequate backups, think the 3-2-1 Rule. Keep at least three backup copies, in two formats and one of those offsite.

Windows

- Apply latest Windows patches and configure automatic security updates.
- Install Sophos Antivirus.
- Enable the windows firewall. Filter access to open ports such as remote desktop.
- Use SSL for all websites. – IT Services offer free SSL Certificates
- Apply a strong password policy. Password should be a minimum 10 characters using a combination of mixed case letters, numbers and symbols. The higher number of characters the stronger the password
- Apply an account lockout policy to prevent brute force attacks.
- Disable unnecessary services.
- Ensure you have adequate backups, think the 3-2-1 Rule. Keep at least three backup copies, in two formats and one of those offsite.

Security Scans

IT Services offer free server security scans using Outpost24 HIAB software.

Security Approval (As owner of the machine you are responsible for information contained on it)	
Confirm that the security standards are in place: (Yes or No)	
Email Address of the registered owner requesting a Outpost24 scans:	

Section G: Scheduling

Requested Implementation Date	Please enter Yes or No
Is this a routine change request?	
Specific date/time request?	
Urgent (i.e. unplanned)? If yes, please explain the reason for urgent change:	

Approval	
Change approved (Yes or No) ?	If yes, by:
Reason for rejection?	

Proposed implementation date\time: _____