**Note some good additional information on security here:** <https://www.titanhq.com/complete-network-security-checklist>

**Security Policy Basics Checklist**

|  |  |
| --- | --- |
| **Requirement** | **Done?** |
| **Firewall configuration** |  |
| Firewall or equivalent in place to protect their internal network and devices against unauthorised access  |  |
| The password on the firewall device should be changed from the default to an alternative strong password  |  |
| **The firewall password is:** |  |
| 1. at least 8 characters long
 |  |
| 1. not the same as the username
 |  |
| 1. does not contain any identical characters next to each other
 |  |
| 1. is not a dictionary word
 |  |
| 1. includes upper and lower case letters, numbers and special characters
 |  |
| 1. has not been reused within a predetermined time period
 |  |
| 1. has not been used for another account
 |  |
| Each rule set on the firewall is authorised and documented including an explanation of the business need for this rule.  |  |
| Unapproved or vulnerable services should be blocked at the gateway firewall  |  |
| Any permissive firewall rules that are no longer required should be disabled as soon as possible  |  |
| The firewall’s boundary administration settings should not be accessible from the internet  |  |
| **Network devices including PC’s & wireless configuration** |  |
| All unnecessary user accounts, guest or admin accounts should be removed or disabled  |  |
| **All user account passwords meet the following requirements:**  |  |
| 1. has been changed from the default password
 |  |
| 1. at least 8 characters long
 |  |
| 1. not the same as the username
 |  |
| 1. does not contain any identical characters next to each other
 |  |
| 1. is not a dictionary word
 |  |
| 1. includes upper and lower case letters, numbers and special characters
 |  |
| 1. has not been reused within a predetermined time period
 |  |
| 1. has not been used for another account
 |  |
| All unnecessary software applications and utilities should be removed or disabled  |  |
| All auto-run features should be disabled including for removable storage media and for network folders  |  |
| An operating systems with integrated desktop firewall should be used on desktop PCs and laptops and configured to block unapproved connections by default. In Windows operating systems from Windows 7 onwards this is built in but needs to be active and configured.  |  |
| **User accounts** |  |
| All users accounts and their privileges should be subject to an approval process and should be documented  |  |
| Admin privileges and any other special access privileges should be restricted to authorised individuals and documented  |  |
| Admin accounts should only be used to perform admin tasks and not for everyday access  |  |
| Admin accounts should be set to require a password change every 60 days or less |  |
| Every individual user should have a unique user name and user account |  |
| **Every user password should meet the following requirements:** |  |
| 1. at least 8 characters long
 |  |
| 1. not the same as the username
 |  |
| 1. does not contain any identical characters next to each other
 |  |
| 1. is not a dictionary word
 |  |
| 1. includes upper and lower case letters, numbers and special characters
 |  |
| 1. has not been reused within a predetermined time period
 |  |
| 1. has not been used for another account
 |  |
| Any user account with special privileges or admin rights should be removed or disabled when no longer required or if the individual changes role or leaves the organisation or after a predefined length of inactivity (eg. if the account is not used for 90 days then it is disabled)  |  |
| **Malware Protection**  |  |
| Malware protection software is to be installed on all computers that can access the internet or are capable of accessing the internet  |  |
|  Malware protection software is to be kept up to date daily  |  |
| Malware protection software should be configured to scan files automatically upon access and to scan web pages when being accessed via a web browser  |  |
| Malware protection software should be configured to perform regular scans of all Files  |  |
| Malware protection software should prevent connections to malicious websites on the internet (e.g. by using website blacklisting).  |  |

|  |  |
| --- | --- |
| **Software Patch Management**  |  |
| Software on any devices that are connected to or are capable of connecting to the internet must be licensed and supported to ensure vulnerabilities are investigated and patches made available.  |  |
| All software updates and security patches that are made available should be installed in a timely manner  |  |
| Any unsupported software should be removed from any computer or device capable of connecting to the internet  |  |
| **Other considerations** |  |
| Wireless Protected Setup (WPS) to be disabled on all wireless devices  |  |
| Universal Plug n Play (UPnP) to be disabled  |  |
| Guest WiFi access to be implemented for visitors and employee owned devices  |  |
| Employee owned devices that can access company email or information will require malware software  |  |
| All network servers must have a daily automated backup solution with backup data stored securely offsite (encrypted)  |  |
| Encryption of all sensitive data stored on mobile devices and removable storage devices  |  |
| Do not allow staff to use file sharing or cloud storage services for company data such as DropBox, OneDrive, Google Drive, iCloud – unless they are authorised by and secured for your organisation.  |  |
| Staff should not be permitted to use personal social media accounts on organisation-owned devices or on any devices connected to the network unless specifically authorised to do so.  |  |