Network Audit Checklist

20 Jun 2023 / BayTechnologies LLC / Dan Michaels

Complete

Score	**95.37%**	Flagged items	**2**	Actions	**1**

Site conducted	Unanswered
Conducted on	20.06.2023 15:58 PST
System Owner	BayTechnologies LLC
Prepared by	Dan Michaels
Site/Location	824 York St Oakland, CA 94610 United States (37.81291031232385, -122.2431947161733)

Flagged items & Actions

2 flagged, 1 action

Flagged items

2 flagged, 0 actions

Network Audit / Computers and Network Devices (including Wireless Access Points and Routers)

• not the same as the username	No

Network Audit / User Accounts

• not the same as the username	No

Other actions

1 action

Network Audit / Firewall

• is not a dictionary word	In Progress

Not a dictionary word but need to change before it’s due for a password change.

To Do | Assignee mailarae o'santos | Priority High | Due 21.06.2023 16:00 PST | Created by SafetyCulture Staff

Firewall password change

Hello Minni, firewall password’s due tomorrow but please change it anytime today. Thank you!

Network Audit

2 flagged, 1 action, 95.37%

Firewall

1 action, 96.15%

The organisation should have a firewall or equivalent in place to protect their internal network and devices against unauthorised access	Yes
The password on the firewall device should be changed from the default to an alternative strong password	Yes

The firewall password is:

• at least 8 characters long	Yes
• not the same as the username	Yes
• does not contain any identical characters next to each other	Yes
• is not a dictionary word	In Progress

Not a dictionary word but need to change before it’s due for a password change.

To Do | Assignee mailarae o'santos | Priority High | Due 21.06.2023 16:00 PST | Created by S afetyCulture Staff

Firewall password change

Hello Minni, firewall password’s due tomorrow but please change it anytime today. Thank you!

• includes upper and lower case letters, numbers and special characters	Yes
• has not been reused within a predetermined time period	Yes
• has not been used for another account	Yes
Each rule set on the firewall must be approved by an authorised individual and documented including an explanation of the business need for this rule.	Yes
Unapproved or vulnerable services should be blocked at the gateway firewall	Yes
Any permissive firewall rules that are no longer required should be disabled as soon as possible	Yes
The firewall’s boundary administration settings should not be accessible from the internet	Yes

Computers and Network Devices (including

1 flagged, 91.67%

Wireless Access Points and Routers)

IMPORTANT: All computers and devices on the network must comply with the following in order to give a 'Yes' response.

All unnecessary user accounts, guest or admin accounts should be removed or disabled	Yes

All user account passwords meet the following requirements:

• has been changed from the default password	Yes
• at least 8 characters long	Yes
• not the same as the username	No
• does not contain any identical characters next to each other	Yes
• is not a dictionary word	Yes
• includes upper and lower case letters, numbers and special characters	Yes
• has not been reused within a predetermined time period	Yes
• has not been used for another account	Yes
All unnecessary software applications and utilities should be removed or disabled	Yes
All auto-run features should be disabled including for removable storage media and for network folders	Yes
An operating systems with integrated desktop firewall should be used on desktop PCs and laptops and configured to block unapproved connections by default. In the latest operating systems, active, and configured.	Yes

User Accounts

1 flagged, 92.31%

All users accounts and their privileges should be subject to an approval process and should be documented	Yes
Admin privileges and any other special access privileges should be restricted to authorised individuals and documented	Yes
Admin accounts should only be used to perform admin tasks and not for everyday access	Yes
Admin accounts should be set to require a password change	Yes

every 60 days or less	
Every individual user should have a unique user name and user account	Yes
Every user password should meet the following requirements:	
• at least 8 characters long	Yes
• not the same as the username	No
• does not contain any identical characters next to each other	Yes
• is not a dictionary word	Yes
• includes upper and lower case letters, numbers and special characters	Yes
• has not been reused within a predetermined time period	Yes
• has not been used for another account	Yes
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)	Yes

Malware Protection

100%

Malware protection software is to be installed on all computers that can access the internet or are capable of accessing the internet	Yes
Malware protection software is to be kept up to date daily	Yes
Malware protection software should be configured to scan files automatically upon access and to scan web pages when being accessed via a web browser	Yes
Malware protection software should be configured to perform regular scans of all files	Yes
Malware protection software should prevent connections to malicious websites on the internet (e.g. by using website blacklisting).	Yes

Software Patch Management

100%

Software on any devices that are connected to or are capable of connecting to the internet must be licensed and supported	Yes

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	Yes
Any unsupported software should be removed from any computer or device capable of connecting to the internet	Yes

Others

100%

Wireless Protected Setup (WPS) to be disabled on all wireless devices	Yes
Universal Plug n Play (UPnP) to be disabled	Yes
Guest WiFi access to be implemented for visitors and employee owned devices	Yes
Employee owned devices that can access company email or information will require malware software	Yes
All network servers must have a daily automated backup solution with backup data stored securely offsite (encrypted)	Yes
Encryption of all sensitive data stored on mobile devices and removable storage devices	Yes
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.	Yes
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.	Yes

Completion

Recommendations

We learned today that we need to be extra careful when giving instructions during trainings particularly when we're giving computer access to avoid the password issue again. We are working to rectify the error by resetting the passwords.

Firewall password reset due tomorrow and is being reset within today.

Name and Signature

Dan Michaels
20.06.2023 16:11 PST