YourIT!
Your Logo Goes Here

Technical Review

Technical Risk Treatment Plan

Prepared for: Client Company

Prepared by: YourIT Company

Table of Contents

Network Management Plan

This ranks individual issues based upon their potential risk to the network while providing guidance on which issues to address by priority. Fixing issues with lower Risk Scores will not lower the Overall Risk Score but will reduce the global Issue Score. To mitigate global risk and improve the health of the network, address issues with higher Risk Scores first.

High Risk

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
97	Upgrade or replace computers with operating systems that are no longer supported. ☐ DESKPC-4PF2ICP / 176.16.1.177 / Windows 10 Pro Version 1909 ☐ DESKPC-09UPSPO / fe80::62:b15d:dc6e:d08d%6,176.16.1.169 / Windows 10 Pro Version 1909	H	H
90	Ensure anti-virus definitions are up to date on specified computers. ☐ Computer: DESKPC-U1K3NAF IP Address: 176.16.1.175 Security Center: Windows Defender ☐ Computer: DESKPC-4PF2ICP IP Address: 176.16.1.177 Security Center: Windows Defender	H	H
90	Ensure anti-spyware definitions are up to date on specified computers. ☐ Computer: DESKPC-U1K3NAF IP Address: 176.16.1.175 Security Center: Windows Defender ☐ Computer: DESKPC-4PF2ICP IP Address: 176.16.1.177 Security Center: Windows Defender	H	H
75	Address patching on computers missing 1-3 security patches. ☐ APPSVR01 / fe80::4183:7729:9818:eb0f%5,176.16.1.14 / Windows Server 2016 Standard	M	H

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
	☐ DCTLR01 / fe80::6168:20a2:860a:bbe0%13,176.16.1.12 / Windows Server 2016 Standard ☐ DESKPC-09UPSPO / fe80::62:b15d:dc6e:d08d%6,176.16.1.169 / Windows 10 Pro Version 1909 ☐ Mac Mini-CServ1 / 176.16.1.5 / Mac macOS 13.2.1 (22D68) ☐ iMac Pro-Mktg1 / 176.16.1.15 / Mac macOS 10.15.7 (19H15)		

Medium Risk

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
68	Free or add additional disk space for the specified drives. ☐ DESKPC-U1K3NAF - C: : 0.03 GB free ☐ DESKPC-4PF2ICP - C: : 0.01 GB free	H	L

Low Risk

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
35	Evaluate the need to have more than 30% of users in the Domain Administrator group and limit administrative access to the minimum necessary. ☐ abwfrcmbr / A Branaugh ☐ ajwfrcmbr / A Jensen ☐ aswfrcmbr / A Smith ☐ Administrator / Administrator ☐ dwfrcmbr / Dora Baxter ☐ dkwfrcmbr / D Kindle ☐ dwwfrcmbr / D White ☐ jswfrcmbr / J Shearing ☐ jwwfrcmbr / J Westerfield ☐ lwwfrcmbr / L Wilson ☐ mgwfrcmbr / M Green ☐ mpwfrcmbr / M Peters ☐ mwwfrcmbr / M Warly	L	M

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
	☐ pkwfrcmbr / P Kettering ☐ pswfrcmbr / P Sulu ☐ skwfrcmbr / S Kulynee ☐ spwfrcmbr / S Photono ☐ thwfrcmbr / T Harris ☐ uwfrcmbr / unitbdr admin ☐ wpwfrcmbr / W Paulson ☐ ydwfrcmbr / Yami Dareloth ☐ ylwfrcmbr / Y Leland		
30	Investigate all accounts with passwords set to never expire and configure them to expire regularly. ☐ MYCO.COM\aswfrcmbr / A Smith ☐ MYCO.COM\dwfrcmbr / Dora Baxter ☐ MYCO.COM\dkwfrcmbr / D Kindle ☐ MYCO.COM\jswfrcmbr / J Shearing ☐ MYCO.COM\jwwfrcmbr / J Westerfield ☐ MYCO.COM\lwwfrcmbr / L Wilson ☐ MYCO.COM\mgwfrcmbr / M Green ☐ MYCO.COM\mpwfrcmbr / M Peters ☐ MYCO.COM\pkwfrcmbr / P Kettering ☐ MYCO.COM\spwfrcmbr / S Photono ☐ MYCO.COM\thwfrcmbr / T Harris ☐ MYCO.COM\ydwfrcmbr / Yami Dareloth ☐ MYCO.COM\ylwfrcmbr / Y Leland ☐ MYCO.COM\ajwfrcmbr / A Jensen ☐ MYCO.COM\dwwfrcmbr / D White ☐ MYCO.COM\mtalman / M Talman ☐ MYCO.COM\mwwfrcmbr / M Warly ☐ MYCO.COM\pswfrcmbr / P Sulu ☐ MYCO.COM\uwfrcmbr / unitbdr admin ☐ MYCO.COM\wpwfrcmbr / W Paulson	L	L
20	Upgrade computers that have operating systems in Extended Support before end of life. ☐ EXCHSVR01 / fe80::c48a:8133:22db:305f%14,fe80::dc13:a1e6:8745:9eb6%12,196.76.48.95,176.16.1.15 / Windows Server 2012 R2 Standard ☐ SQLSVR01 / fe80::5072:f78c:9e73:a130%12,176.16.1.17 / Windows Server 2012 R2 Standard ☐ DESKPC-RB3LBP3 /	L	L

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
	fe80::3196:5fc5:f131:a6b0%2,176.16.1.181 / Windows 10 Enterprise 2015 LTSB		
15	Investigate the list of inactive computers and determine if they should be removed from Active Directory, rejoined to the network, logged into by authorized users, or powered on. ☐ WRKSTN7-2 / 176.16.1.115 / Windows 10 Pro Version 1909 ☐ WRKSTN10-3 / 176.16.1.141 / Windows 10 Enterprise ☐ WRKSTN8-1 / 176.16.1.128 / Windows 10 Pro Version 1909 ☐ WS2012SVR / 176.16.1.135 / Windows Server 2012 Standard Evaluation ☐ WRKSTN8-4 / 176.16.1.137 / Windows 10 Pro Version 1909 ☐ WRKSTN7-1 / 176.16.1.126 / Windows 10 Professional 1909 ☐ DESKPC-MJOD0L9 / 176.16.1.120 / Windows 10 Enterprise ☐ DESKPC-MGMT01 / 176.16.1.113 / Windows 10 Enterprise ☐ RFHVNDA1 / 176.16.1.11 / Windows Server 2016 Standard ☐ WRKSTN8-3 / 176.16.1.136 / Windows 10 Pro Version 1909 ☐ WRKSTN8-2 / 176.16.1.131 / Windows 10 Pro Version 1909 ☐ BDR01 / 176.16.1.140 / Windows Server 2016 Standard		
13	Disable or remove user accounts for users that have not logged on to active directory in 30 days. ☐ ajwfrcmbr / A Jensen ☐ arom / Axel Rom ☐ Administrator / Administrator ☐ dwwfrcmbr / D White ☐ ebaldwin / Edward Baldwin ☐ fowardslash / fowared slash ☐ jknightling / Jorge Knightling ☐ jasus / Jeremy Asus ☐ jgilligan / Julia Gilligan ☐ jkalo / Jessica Kalo ☐ jchestnut / Janet Chestnut		

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY

- ☐ jconway / Joseph Conway
- ☐ jdelaney / Jonah Delaney
- ☐ mwwfrcmbr / M Warly
- ☐ mjohnson / Maxwell Johnson
- ☐ mtalman / M Talman
- ☐ pwalker / Paula Walker
- ☐ pswfrcmbr / P Sulu
- ☐ sjane / Sonny Jane
- ☐ tshelman / Terri Shelman
- ☐ uwfrcmbr / unitbdr admin
- ☐ wpwfrcmbr / W Paulson

Security Management Plan

This ranks individual issues based upon their potential risk to the network while providing guidance on which issues to address by priority. Fixing issues with lower Risk Scores will not lower the Overall Risk Score but will reduce the global Issue Score. To mitigate global risk and improve the health of the network, address issues with higher Risk Scores first.

High Risk

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
95	Assess the risk of each vulnerability and remediate all external vulnerabilities as prescribed. ☐ Name: Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater) / CVSS: 7.5 / IP: 96.67.119.196	H	H
77	Enable account lockout for all users.	H	H
75	Assess the risk of each vulnerability and remediate all external vulnerabilities as prescribed. ☐ Name: SSL/TLS: Missing `secure` Cookie Attribute / CVSS: 6.4 / IP: 96.67.119.196 ☐ Name: SSL/TLS: BREACH attack against HTTP compression / CVSS: 5.9 / IP: 96.67.119.196 ☐ Name: SSL/TLS: Certificate Expired / CVSS: 5 / IP: 96.67.119.196 ☐ Name: Missing `httpOnly` Cookie Attribute / CVSS: 5 / IP: 96.67.119.196	H	H
72	Enable automatic screen lock on the specified computers. ☐ APPSVR01 ☐ DCTLR01 ☐ DCTLR02 ☐ EXCHSVR01 ☐ FSSVR01 ☐ HVSVR1 ☐ SQLSVR01	M	M

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
	☐ SQLSVR02		

YourIT!
Your Logo Goes Here

Data Security Management Plan

This ranks individual issues based upon their potential risk to the network while providing guidance on which issues to address by priority. Fixing issues with lower Risk Scores will not lower the Overall Risk Score but will reduce the global Issue Score. To mitigate global risk and improve the health of the network, address issues with higher Risk Scores first.

High Risk

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
87	Access by users marked as "Not Authorized" who have attempted to or successfully logged into a computer with PII should be investigated to see if a breach has occurred. ☐ msimpson : M Simpson ☐ yslobedin : Y Slobedin	H	H
87	Access by users marked as "Not Authorized" who have attempted to or successfully logged into a computer with ePHI should be investigated to see if a breach has occurred. ☐ pralston : P Ralston ☐ jsmith : J Smith	H	H
87	Access by users marked as "Not Authorized" who have attempted to or successfully logged into a computer with PCI Cardholder Data should be investigated to see if a breach has occurred. ☐ ahollings : A Hollings ☐ srogers : S Rogers ☐ ttrundle : T Trundle	H	H
80	Investigate the unauthorized computers storing GDPR Personal Data. Personal Data should be stored on computers in accordance with organization policy. ☐ WRKSTN10-4 / 176.16.1.133	H	H

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
80	Investigate the unauthorized computers storing ePHI. ePHI should be stored on computers in accordance with organization policy. ☐ DESKPC-35EGQCC / 176.16.1.79 ☐ DESKPC-BDJFFLG / 176.16.1.63 ☐ DESKPC-F6CKERQ / 176.16.1.59		
80	Investigate the unauthorized computers storing PII. PII should be stored on computers in accordance with organization policy. ☐ DESKPC-35EGQCC / 176.16.1.79 ☐ DESKPC-BDJFFLG / 176.16.1.63 ☐ DESKPC-F6CKERQ / 176.16.1.59 ☐ WRKSTN10-1 / 176.16.1.138 ☐ WRKSTN10-4 / 176.16.1.133		
80	Investigate the network shares authorized to store Sensitive Data with unrestricted access. Limit access to the minimum necessary. ☐ \\FSSVR01\Accounting : D:\Shares\Accounting ☐ \\FSSVR01\Human Resources : D:\Shares\Human Resources ☐ \\FSSVR01\Operations : D:\Shares\Operations		
78	Ensure that data is properly backed up on computers with GDPR Personal Data. See the Asset Inventory Worksheet for a list of computers that are documented as not having a backup agent installed. ☐ WRKSTN10-4 / 176.16.1.133		
78	Ensure that data is properly backed up on computers with PII. See the Asset Inventory Worksheet for a list of computers that are documented as not having a backup agent installed. ☐ DESKPC-35EGQCC / 176.16.1.79 ☐ DESKPC-BDJFFLG / 176.16.1.63 ☐ DESKPC-F6CKERQ / 176.16.1.59		

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
	☐ FSSVR01 / 176.16.1.161 ☐ WRKSTN10-1 / 176.16.1.138 ☐ WRKSTN10-4 / 176.16.1.133		
78	Ensure that data is properly backed up on computers with ePHI. See the Asset Inventory Worksheet for a list of computers that are documented as not having a backup agent installed. ☐ DESKPC-35EGQCC / 176.16.1.79 ☐ DESKPC-BDJFFLG / 176.16.1.63 ☐ DESKPC-F6CKERQ / 176.16.1.59 ☐ FSSVR01 / 176.16.1.161		
75	Implement disk encryption on computers storing ePHI. ☐ DESKPC-35EGQCC / 176.16.1.79 ☐ DESKPC-BDJFFLG / 176.16.1.63 ☐ DESKPC-F6CKERQ / 176.16.1.59 ☐ FSSVR01 / 176.16.1.161		
75	Implement disk encryption on computers storing GDPR Personal Data. ☐ WRKSTN10-4 / 176.16.1.133		
75	Implement disk encryption on computers storing PII. ☐ DESKPC-35EGQCC / 176.16.1.79 ☐ DESKPC-BDJFFLG / 176.16.1.63 ☐ DESKPC-F6CKERQ / 176.16.1.59 ☐ FSSVR01 / 176.16.1.161 ☐ WRKSTN10-1 / 176.16.1.138 ☐ WRKSTN10-4 / 176.16.1.133