|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  | pic455 |  |  |
| pic456 |  |  |  |  |
|  | |  | | --- | | **TECHNICAL RISK TREATMENT PLAN** | |  |  |  |
|  | COBAIT |  | |  | | --- | | Prepared for:  **HHER - GALVESTON**  12/09/2024 | |  |
|  | |  | | --- | | COMPANY STATE | COMPANY PHONE | COMPANY EMAIL | COMPANY WEBSITE URL | |  |  |  |
|  | |  | | --- | | CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way. | |  |  |  |
|  |  |  |  |  |

# Table of Contents

|  |  |  |
| --- | --- | --- |
| **01** |  | [Network Management Plan](#nmp) |

|  |  |  |
| --- | --- | --- |
| **02** |  | [Security Management Plan](#smp) |

|  |  |  |
| --- | --- | --- |
| **03** |  | [Data Security Management Plan](#dsmp) |

# 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.

|  |  |
| --- | --- |
| pic457 | High Risk |

| Risk Score | Recommendation | Severity | Probability |
| --- | --- | --- | --- |
| **97** | Upgrade or replace computers with operating systems that are no longer supported.   🗆 HHER-NBPC01 / 10.0.1.107 / Windows 10 Pro Version 21H2  🗆 HHER-NBPC18 / 10.0.1.116 / Windows 10 Pro Version 21H2  🗆 HHGALV-COV-LPT2 / fe80::195b:d363:ee7d:a12d%16,10.1.3.172 / Windows 10 Pro Version 1903  🗆 HHGALV-PC05 / fe80::1f90:6364:dfbe:28f9%18,10.1.3.142 / Windows 10 Pro Version 21H2  🗆 HHGALV-PC07A / ::1,10.1.3.155 / Windows 10 Pro Version 21H2  🗆 HHGALV-PC08 / fe80::571d:df50:c6bd:7011%2,10.1.3.156 / Windows 10 Pro Version 21H2  🗆 HHGALV-PC10 / fe80::a226:d75c:b7e9:b63%4,10.1.3.145 / Windows 10 Pro Version 21H2  🗆 HHGALV-PC11 / fe80::1827:7c18:3255:6988%11,10.1.3.144 / Windows 10 Pro Version 21H2  🗆 HHGALV-PC12 / fe80::2eb7:627a:4cb0:e5a7%6,10.1.3.90 / Windows 10 Pro Version 21H2  🗆 HHLNV-HOSP02 / 10.0.1.158 / Windows 11 Pro Version 22H2  🗆 HHLNV-HOSP04 / 10.0.1.142 / Windows 10 Pro Version 21H2  🗆 HHLNV-HOSP05 / 10.0.1.101 / Windows 10 Pro Version 21H2  🗆 HHLNV-HOSP10 / 10.0.1.143 / Windows 10 Pro Version 21H2  🗆 HHLNV-HOSP15 / 10.0.1.87 / Windows 10 Pro Version 21H2  🗆 HHLNV-HOSP16 / 10.0.1.160 / Windows 10 Pro Version 21H2  🗆 HHLNV-PC1 / 10.0.1.196 / Windows 10 Pro Version 21H2  🗆 HHLNV-PC4 / 10.0.1.181 / Windows 10 Pro Version 1803  🗆 HHLW-PC2 / 10.0.1.176 / Windows 10 Pro Version 21H2  🗆 RADCT-TRAILER / 10.0.1.171 / Windows 10 Pro Version 21H2  🗆 SCRIPTRXLNV-PC / 10.0.1.166 / Windows 10 Pro Version 21H2  🗆 SVR02 / 10.0.1.11 / Windows Server 2012 R2 Standard | pic458 | pic459 |
| **94** | Assure that anti-spyware is deployed to all possible endpoints in order to prevent both security and productivity issues.   🗆 Computer: HHGALV-PC06 IP Address: 10.1.3.89  🗆 Computer: HHLNV-HOSP11 IP Address: 10.0.1.201 | pic460 | pic461 |
| **90** | Ensure anti-spyware definitions are up to date on specified computers.   🗆 Computer: HHGALV-PC01 IP Address: 10.1.3.197 Security Center: Windows Defender  🗆 Computer: HHLNV-ANNEX IP Address: 10.0.1.190 Security Center: Windows Defender | pic462 | pic463 |

|  |  |
| --- | --- |
| pic464 | Low Risk |

| Risk Score | Recommendation | Severity | Probability |
| --- | --- | --- | --- |
| **30** | Investigate all accounts with passwords set to never expire and configure them to expire regularly.   🗆 HHER.LCL\Cam.User / Cam User  🗆 HHER.LCL\Charge.Nurse / Charge Nurse  🗆 HHER.LCL\cobaitadmin / Cobait Admin  🗆 HHER.LCL\HHLNV.LAB / HHLNV LAB  🗆 HHER.LCL\HHLNV.LAB3 / HHLNV LAB3  🗆 HHER.LCL\lisadmin / LIS ADMIN  🗆 HHER.LCL\scriptrx / Script Rx  🗆 HHER.LCL\Staff.view / staffview  🗆 HHER.LCL\Ultrasound / Ultrasound  🗆 HHER.LCL\CBTAdmin / COBAIT Temp Admin  🗆 HHER.LCL\ccadmin / CC Admin  🗆 HHER.LCL\HHLNV.LAB2 / HHLNV LAB2.  🗆 HHER.LCL\hhlw / hhlw  🗆 HHER.LCL\labscan / lab scan  🗆 HHER.LCL\labscans / labscans  🗆 HHER.LCL\long.helpdesk / Long Helpdesk Support  🗆 HHER.LCL\Medsupply / MedSupply  🗆 HHER.LCL\NOCAdmin / NOCAdmin  🗆 HHER.LCL\radtech / radtech  🗆 HHER.LCL\RDPScriptRX / RDP Scriptrx  🗆 HHER.LCL\scan.user / Scan User  🗆 HHER.LCL\stasis.lab / Stasis Lab  🗆 HHER.LCL\tyl.helpdesk / Tyler Helpdesk Support | pic465 | pic466 |
| **20** | Upgrade computers that have operating systems in Extended Support before end of life.   🗆 HHGALV-SRXSVR / fe80::2c17:808e:79e6:3728%4,10.1.3.11 / Windows Server 2016 Standard  🗆 HHGALV-DC01 / ::1,10.1.3.10 / Windows Server 2016 Standard  🗆 HHLNV-LAB-APP / 172.16.0.51 / Windows Server 2019 Standard  🗆 HHLNV-LAB-DB / 172.16.0.50 / Windows Server 2019 Standard  🗆 HHGALV-FS01 / fe80::f8af:682d:8a5e:ec4e%2,10.1.3.12 / Windows Server 2016 Standard  🗆 HHLNV-FS01 / 10.0.1.12 / Windows Server 2019 Standard  🗆 HHLNV-SRXSVR / 10.0.1.82,10.0.1.13 / Windows Server 2016 Standard | pic467 | pic468 |
| **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.   🗆 SVRBK / 10.0.1.12 / Windows Server 2012 R2 Standard  🗆 HHLNV-LT08 / 172.16.1.212 / Windows 10 Pro  🗆 HHLNV-LT12 / 10.0.5.145 / Windows 10 Pro  🗆 HHLVN-HOSP-LT2 / 172.16.3.123 / Windows 10 Pro  🗆 HHERLNV-LT15 / 172.16.2.28 / Windows 10 Pro  🗆 HHGALV-LTMD / 10.1.3.81 / Windows 11 Pro | pic469 | pic470 |
| **13** | Disable or remove user accounts for users that have not logged on to active directory in 30 days.  100 of 623 displayed. See Technical Risk Treatment Plan Details.xlsx report generated in Excel format.   🗆 Aaron.Love / Aaron Love  🗆 Abbey.Redding / Abbey Redding  🗆 abbigalle.anderson / Abbigalle Anderson  🗆 Abigail.Avelar / Abigail Avelar  🗆 Abigail.Ervin / Abigail Ervin  🗆 adam.corley / Adam Corley  🗆 Adia.Holmes / Adia Holmes  🗆 Administrator / Administrator  🗆 Adriana.Griffin / Adriana Griffin  🗆 Aimee.Moore / Aimee Moore  🗆 Ajitha.Raju / Ajitha Raju  🗆 alex.lawrence / Alex Lawrence  🗆 alex.marshall / Alex R. Marshall  🗆 Alexa.Fleming / Alexa Fleming  🗆 Alexandra.ferro / Alexandra Ferro  🗆 Alexandria.Longoria / Alexandria Longoria-Lopez  🗆 Alexandria.Mason / Alexandria Mason  🗆 Alexis.Arocha / Alexis Arocha  🗆 Alexis.Mars / Alexis Mars  🗆 alexis.villarreal / Alexis Villarreal  🗆 alexus.wilson / Alexus Wilson  🗆 alice.williams / Alice Williams  🗆 Alieca.McCann / Alieca McCann  🗆 Alishia.Burse / Alishia Burse  🗆 alison.delarosa / Alison DeLaRosa  🗆 Allen.Reaves / Allen  🗆 Allie.Chesney / Allie Chesney  🗆 $DUPLICATE-1dbf / Alonso Osorio  🗆 alonso.osorio / Alonso Osorio  🗆 Alyson.Kipp / Alyson Kipp  🗆 Alyssa.Earl / Alyssa Earl  🗆 ALear / Alyssa Lear  🗆 Alyssa.Threadgill / Alyssa Threadgill  🗆 Amanda.Bickham / Amanda Bickham  🗆 amanda.brauer / Amanda Brauer  🗆 Amanda.Viehmann / Amanda Viehmann  🗆 amber.herrington / Amber Herrington  🗆 amber.key / Amber Key  🗆 Amy.Bradbery / Amy Bradbery  🗆 Amy.Fajardo / Amy Fajardo  🗆 agillaspy / Amy Gillaspy  🗆 Amy.Harding / Amy Harding  🗆 Amy.Polve / Amy Polve  🗆 Amy.Wood / Amy Wood  🗆 andrea.boyd / Andrea Boyd  🗆 andres.galindo / Andres Galindo  🗆 Andrew.Kerman / Andrew Kerman  🗆 Andy.Kerman / Andy Kerman  🗆 Angela.Jacquez / Angela Jacquez  🗆 Angela.Norman / Angela Norman  🗆 angela.smith / Angela Smith  🗆 Angela.Sanders / Angela.Sanders  🗆 Angie.McInnis / Angie McInnis  🗆 Annalyn.Moore / Annalyn Moore  🗆 anthony.rowe / Anthony Rowe  🗆 April.Helms / April Conrad-Helms  🗆 april.young / April Young  🗆 Ariel.Snow / Ariel Snow  🗆 ashley.dispenza / Ashley Dispenza  🗆 Ashley.Hooser / Ashley Hooser  🗆 Ashley.Peterson / Ashley Peterson  🗆 Ashley.Turner / Ashley Turner  🗆 ashten.littlefield / Ashten Littlefield  🗆 Audri.Clements / Audri Clements  🗆 Aurora.Gutierrez / Aurora Gutierrez  🗆 Austin.Henigan / Austin Henigan  🗆 Azucena.San.Juan / Azucena San Juan  🗆 bailey.jones / Bailey Jones  🗆 Banita.Galimore / Banita Galimore  🗆 baylee.martin / Baylee Martin  🗆 Beatriz.Sheets / Beatriz Sheets  🗆 belinda.daniel / Belinda Daniels  🗆 belinda.pryor / Belinda Pryor  🗆 Ben.Constante / Ben Constante  🗆 Berenice.schuler / Berenice schuler  🗆 bethany.starks / Bethany Starks  🗆 Bobby.Grffith / Bobby Grffith  🗆 bstarling / Bonita Starling  🗆 byoung / Brad Young  🗆 Brandi.Love / Brandi Love  🗆 bmeter / Brandi V. Meter  🗆 BrandiJo.Smith / BrandiJo Smith  🗆 Breanna.Taves / Breanna Taves  🗆 Bri.Richardson / Bri Richardson  🗆 Brian Corley / Brian Corley  🗆 brian.johns / Brian Johns  🗆 Brianna.Cuyos / Brianna Cuyos  🗆 brianne.powell / Brianne Powell  🗆 brittany.Feagins / Brittany Feagins  🗆 Brittany.McGuire / Brittany McGuire  🗆 brooke.green / Brooke Green  🗆 $DUPLICATE-fe6 / Brooke Taylor  🗆 brooke.taylor / Brooke Taylor  🗆 Brooke.Whitfield / Brooke Whitfield  🗆 brooke.woods / Brooke Woods  🗆 Brooklyn.Potts / Brooklyn Potts  🗆 cace.hurt / Cace Hurt  🗆 Camela.Miller / Camela Miller  🗆 Candes.Kelley / Candes Kelley  🗆 candice.glasco / Candice Glasco | pic471 | pic472 |
| **10** | There may be a legitimate business need, but these risks should be assessed individually. Certain protocols are inherently insecure since they often lack encryption. Inside the network, their use should be minimized as much as possible to prevent the spread of malicious software. Of course, there can be reasons these services are needed and other means to protect systems which listen on those ports. We recommend reviewing the programs listening on the network to ensure their necessity and security. See Listening Ports sheets in Excel Export for details.    🗆 Unknown Device Name (10.1.3.194) - Listening ports: 5900  🗆 Unknown Device Name (10.1.3.210) - Listening ports: 5900  🗆 Unknown Device Name (10.1.3.211) - Listening ports: 5900  🗆 Unknown Device Name (10.1.3.212) - Listening ports: 5900  🗆 Unknown Device Name (10.1.3.213) - Listening ports: 5900  🗆 Unknown Device Name (10.1.3.250) - Listening ports: 23  🗆 Unknown Device Name (10.1.3.251) - Listening ports: 23 | pic473 | pic474 |

# 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.

|  |  |
| --- | --- |
| pic475 | High Risk |

| Risk Score | Recommendation | Severity | Probability |
| --- | --- | --- | --- |
| **77** | Enable account lockout for all users.   🗆 HHGALV-COV-LPT2  🗆 HHGALV-DC01  🗆 HHGALV-FS01  🗆 HHGALV-PC03  🗆 HHGALV-PC04  🗆 HHGALV-PC05  🗆 HHGALV-PC07A  🗆 HHGALV-PC08  🗆 HHGALV-PC09  🗆 HHGALV-PC09NS  🗆 HHGALV-PC10  🗆 HHGALV-PC11  🗆 HHGALV-PC12  🗆 HHGALV-SRXPC01  🗆 HHGALV-SRXSVR | pic476 | pic477 |
| **75** | Enable enforcement of password length to 8 or more characters.   🗆 HHGALV-COV-LPT2  🗆 HHGALV-DC01  🗆 HHGALV-FS01  🗆 HHGALV-PC03  🗆 HHGALV-PC04  🗆 HHGALV-PC05  🗆 HHGALV-PC07A  🗆 HHGALV-PC08  🗆 HHGALV-PC09  🗆 HHGALV-PC09NS  🗆 HHGALV-PC10  🗆 HHGALV-PC11  🗆 HHGALV-PC12  🗆 HHGALV-SRXPC01  🗆 HHGALV-SRXSVR | pic478 | pic479 |
| **72** | Enable automatic screen lock on the specified computers.   🗆 HHGALV-COV-LPT2  🗆 HHGALV-DC01  🗆 HHGALV-FS01  🗆 HHGALV-PC03  🗆 HHGALV-PC04  🗆 HHGALV-PC05  🗆 HHGALV-PC07A  🗆 HHGALV-PC08  🗆 HHGALV-PC09  🗆 HHGALV-PC09NS  🗆 HHGALV-PC10  🗆 HHGALV-PC11  🗆 HHGALV-PC12  🗆 HHGALV-SRXPC01  🗆 HHGALV-SRXSVR | pic480 | pic481 |

|  |  |
| --- | --- |
| pic482 | Medium Risk |

| Risk Score | Recommendation | Severity | Probability |
| --- | --- | --- | --- |
| **~~70~~** | Modify the maximum password age to be 90 days or less. | pic483 | pic484 |

|  |  |
| --- | --- |
| pic485 | Low Risk |

| Risk Score | Recommendation | Severity | Probability |
| --- | --- | --- | --- |
| **50** | Ensure company's WiFi is secure and discourage the use of any open WiFi connections.   🗆 Insecure Wireless - xfinitywifi  🗆 Insecure Wireless - Hilton Honors Home2  🗆 Insecure Wireless - Hilton Honors Tru  🗆 Insecure Wireless - CableWiFi | pic486 | pic487 |

# 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.

|  |  |
| --- | --- |
| pic488 | Low Risk |

| Risk Score | Recommendation | Severity | Probability |
| --- | --- | --- | --- |
| **50** | Reduce or eliminate the use of USB drives in the environment.   🗆 HHGALV-PC03 - E: USB SanDisk 3.2Gen1 USB Device | pic489 | pic490 |