***Risk Register for Regional Gardens Ltd***

| Risk | Impact | Inherent Risk | Controls | Residual Risk | Priority |
| --- | --- | --- | --- | --- | --- |
| No education and awareness training | Medium | Medium | Implement Information Security education and awareness training for all staff. [1] | Low | Medium |
| Staff have administrator privileges on their own workstations | Medium | High | Restrict administrator privileges to system administrators [1] | Low | High |
| No Multi-factor authentication | Medium | Medium | Implement Multi-factor authentication [2] | Low | Medium |
| Shared/Duplicate Administrator Passwords | High | High | Need to implement password policy for strong, unique passwords [3,1] | Low | High |
| Free, open unrestricted access to the internet for all employees | Medium | Medium | At a minimum block malicious domains, restrict access to non-work related sites. [4] | Low | Medium |
| Idle but active user accounts | Medium | Medium | Remove active but unused accounts and implement as part of off-boarding proceedure [1] | Low | High |
| External originating emails | Medium | Medium | Enable email flagging so staff can easily identify emails from external sources and exercise appropriate caution [4] | Low | Low |
| No PCI/DSS (payment card industry data security standard) policy |  |  | Develop a PCI/DSS policy to standards [3] |  |  |
| No Access Control policy |  |  | Develop an Access Control policy [3] |  |  |
| No Password policy |  |  | Develop a Password policy [3] |  |  |
| No Incident Response plan |  |  | Develop an Incident Response plan [3] |  |  |
| No Business Continuity plan |  |  | Develop a Business Continuity plan [3] |  |  |
| No Crisis Management plan |  |  | Develop a Crisis Management plan [3] |  |  |
| No Backup policy |  |  | Develop a backup policy [3] |  |  |
| Adhoc Patching and updates policy |  |  | Develop a Patching and Updates policy [3] |  |  |
| No On-boarding / Off-boarding policy |  |  | Develop an On-boarding Off-boarding policy [3] |  |  |
| No BYOD (Bring your own device) policy |  |  | Develop a BYOD policy [3] |  |  |
| No remote access policy |  |  | Develop a remote access policy [3] |  |  |
| No cyber-insurance |  |  | Shop for an applicable cyber-insurance policy |  |  |
|  |  |  | Buy or block typo-squatted domains [4] |  |  |
| Active Directory Servers - Operating System not patched and OS Windows Server 2008 R2 support to end 14th Jan 2020 [5] |  |  | Upgrade to current version Windows Server 2019 |  |  |
| SQL Servers - Operating System not patched and OS depricated Windows Server 2003 support ended 14th July 2015 [6] |  |  | Upgrade to current version Windows Server 2019 |  |  |
| SQL Servers - Deprecated SQL Server 2003 support ended 14th July 2015 [7] |  |  | Upgrade to current version SQL Server 2016 |  |  |
| Exchange Email Server - Operating System not patched and OS Windows Server 2008 R2 support to end 14th Jan 2020 [5] |  |  | Upgrade to current version Windows Server 2019 |  |  |
| Exchange Email Server - Exchange 2007 end of life 11th April 2017 [8] |  |  | Upgrade to current version Exchange 2016 |  |  |
| File and Print Servers - Operating System not patched and OS depricated Windows Server 2003 support ended 14th July 2015 [7] |  |  | Upgrade to current version Windows Server 2019 |  |  |
|  |  |  |  |  |  |
| Red Hat Enterprise Servers - Operating System not patched and OS depricated Red Hat 5 Enterprise support ended 31st March 2017 [9] |  |  | Upgrade to current version Red Hat 7.6 |  |  |
| Workstations - Operating System not patched and OS Windows 7 support to end 14th Jan 2020 [10] |  |  | Upgrade to current version Windows 10 before 14th Jan 2020 |  |  |
| Servers – Anti-virus not updated |  |  | Install Anti-virus software and update as per new update policy [1] |  |  |
| Workstations – Anti-virus not updated |  |  | Install Anti-virus software and update as per new update policy. Recommend enabling automatic updates [1] |  |  |
| Macbooks – No Anti-virus installed |  |  | Install Anti-virus software and update as per new update policy. Recommend enabling automatic updates [1] |  |  |
| Software – no maintenance contracts for installed software |  |  |  |  |  |
| All operating systems – none of the machines have undergone any type of operating system hardening |  |  | Harden all end-points to recommended standards  [1] |  |  |
| No Event logging or monitoring |  |  | Buy a SIEM (security information and event management) solution [1] |  |  |
| No email virus protection |  |  | Implement email anti-virus solution on mail servers [1] |  |  |
| Servers - >5 year old hardware must be close to Mean Time to Failure (MTTF) [1] |  |  | Replace with new hardware |  |  |
|  |  |  |  |  |  |
| Workstations - >5 year old hardware must be close to Mean Time to Failure (MTTF) [1] |  |  | Replace with new hardware |  |  |
| Servers and networking hardware - Servers located in common area – easy to steal or infect with malware etc |  |  | Needs separate area for servers and network hardware, able to control heat, dust, humidity. Kept locked with keys only available to those authorised [1] |  |  |
| No maintenance contract for hardware |  |  |  |  |  |
| No disk redundancy in servers |  |  | Upgrade to new servers capable of a Raid Solution with sufficient storage capacity [1] |  |  |
| 10mb Hubs - Allow for anyone connected to the network to sniff all network traffic [] |  |  | Replace with Switches |  |  |
| No Firewall |  |  | Purchase an appropriate Firewall or similar gateway security device [1] |  |  |
| Servers on the same network as workstations, no depth of defence |  |  | Reorganise the network topology into Vlans or subnets [1] |  |  |
| ADSL- there is only one ADSL connection (no redundancy) |  |  | Get at least a second internet connection from a different provider to serve as both back-up and load-balancing functions |  |  |
| Network Availability – No D/DoS Mitigation |  |  | Outsource a D/Dos solution or talk with internet service providers to see if they offer the service [11] |  |  |
| All servers have publicly accessible internet addresses |  |  | Limit outside internet accessibility to authorised parties only documented in newly formed access control / remote access policy [1] |  |  |

References

[1] D. L. Prowse, “CompTIA Security+ SYO-501 Cert Guide: Fourth Edition” Pearson Education Inc, 2018.

[2] C. P. Pfleeger, and S. L. Pfleeger, “Security in Computing: Fourth Edition” Prentice Hall, 2007.

[3] M. E. Whitman and H. J. Mattord, “Management of Information Security: Sixth Edition” Cenage Learning, Inc, 2019.

[4] C. Ford, “A Hacker, I Am” Craig Ford, 2019

[5] Microsoft, “Prepare for Windows Server 2008 end of support” Microsoft.com

<https://www.microsoft.com/en-au/cloud-platform/windows-server-2008> (accessed Jan. 5, 2020)

[6] Microsoft, “Running Windows Server 2003 on Microsoft Azure” Microsoft.com

<https://support.microsoft.com/en-au/help/4010166/running-windows-server-2003-on-microsoft-azure> (accessed Jan. 5, 2020)

[7] Microsoft, “Search product lifecycle” Microsoft.com

<https://support.microsoft.com/en-au/lifecycle/search/1044> (accessed Jan. 5, 2020)

[8] Microsoft, “Exchange 2007 end of support roadmap” Microsoft.com

<https://docs.microsoft.com/en-us/office365/enterprise/exchange-2007-end-of-support> (accessed Jan. 5, 2020)

[9] Red Hat, “FAQ: Red Hat Enterprise Linux 5 Reaches End of Full/Maintenance Phases and Transitions to Extended Life Phase” Redhat.com <https://access.redhat.com/articles/2986371> (accessed Jan. 5, 2020)

[10] Microsoft, “Windows 7 support will end on January 14, 2020” Microsoft.com

<https://support.microsoft.com/en-au/help/4057281/windows-7-support-will-end-on-january-14-2020> (accessed Jan. 5, 2020)

[11] E. Chou and R. Groves, “Distributed Denial of Service (DDoS): Practical Detection and Defence” O’Reilly Media Inc, 2018