 Regional Gardens Ltd Data Integrity Policy

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Approved by | Approval date | Effective date | Next Review |
| 1.0 | Chief Information Officer | 19 January 2020 | 19 January 2020 | March 2020 |

This Policy also refers to the following documents:

|  |
| --- |
| Access Control Policy |
| Password Policy |
| Acceptable Use Policy |
| Patching and Updates Policy |
| BYOD Policy |
| On-Boarding, Off-Boarding Policy |
| Incident Response Plan |
| Disaster Recovery Plan |
| Business Continuity Plan |
|  |

1. Brief Overview

Preserving the integrity of the company data is critical for maintaining business continuity. There is a great risk environment for small business, with the recent increase in both ransomware attacks and data breaches coupled with the fact that these businesses are attractive targets for criminals as they have more data and assets than consumers but generally less security than larger business [1,2]. Something as simple as accidental alteration of current stock levels or stock prices could result in considerable financial loss [3]. This is a policy to protect and preserve Regional Gardens Ltd electronic data against unauthorised alteration, deletion or modification from accidental, malicious, internal or external sources [4,5].

2. Policy Purpose and Rationale

The intent of this policy is to formulate company specific best practises to provide a solid framework to protect the various data sets by providing integrity, non-repudiation, authenticity, auditability and accountability. To define roles & responsibilities, ensure legal and regulatory compliance is met and to outline procedures for data retention and destruction.

3. Policy Scope

This Data Integrity Policy applies to all employees of Regional Gardens Ltd. It includes but is not limited to all data required in the day to day operation of Regional Gardens Ltd. comprising the following electronic data sets: Nursery product data, Nursery supplies data, Strategic planning data, Customer planning data, Personnel data, Web page data, Email, Corporate finance data, other Customer related data and associated Corporate intellectual property data.

4. Roles and Responsibilities

|  |  |
| --- | --- |
| Role | Responsibilities |
| Management | The primary tasks for management are policy enforcement, fostering a security culture of open reporting, maintaining the strategic planning data and approving policy and controls [7]. |
| Chief Information Officer | Overseeing management of the data, validating and evaluating the effectiveness of associated security controls and keeping the policy updated [7]. |
| Data Owners | The creator of the data is responsible for accurate entries [4] and maintaining quality of data. Ensure the minimum, workable volume of business data is kept [1]. |
| Data Custodians | The system administrators are responsible for maintaining integrity of all data, initiating incremental weekly backups & testing recovery procedures. They are likewise tasked with updating software to reduce risk and checking audit logs. Ensure the minimum, workable volume of business data is kept [1]. |
| Data Users | Data Users are responsible for accurate entries and edits [4]. Reporting any noticeable discrepancies and not to circumvent data integrity controls. They are responsible for their own composed email and not divulging any company data usage as per acceptable use policy [5,6,7]. Ensure the minimum, workable volume of business data is kept [1]. |
| Employees | |
| Nursery Staff | Nursery product and supplies data |
| Regional Gardens Planning | customer planning data |
| Human Resources | personnel data, on-boarding, off-boarding policy adhered to |
| Finance | corporate finance data |
| Administration | personnel data |

5. Mandatory Requirements

5.1 Data classification scheme - Public, confidential, sensitive, top-secret [4]. Data Owner to maintain control over shared data [1]. Data files must only be able to be modified by authorised users using Role Based Access Control, using mechanisms of Least Privilege and Implicit Deny as outlined in the Access Control policy [4,5,6].

5.2 Encryption - All data is to be encrypted in storage, in transit and in use. Hashes or digital signatures of data files need to be created so that modification is cryptographically detectable.

5.3 Anti-virus – Anti-virus must be installed on all workstations, mobile devices and servers and kept updated. Real-time protection must be enabled for workstations and virus scan on boot, with system administrators to virus scan servers daily [1]. All incoming and outgoing emails are to be scanned for viruses.

5.4 Backups and recovery – System Administrators are to take daily snapshots of critical systems, and schedule weekly incremental backups. The Disaster recovery plan and backups must be thoroughly tested to ensure they work when required [1,2,4,5,6]. A combination of cloud and or multiple secure off-site backups must be organised for redundancy and to limit unauthorised access [2].

5.5 Data archiving, retention and destruction – It is a legal requirement that corporate finance data be kept for 7 years for taxation audit requirements. The disposal of old backup media is to be outsourced to an accredited document destruction company [2]. Ensure the minimum, workable volume of business data is kept, and limit the amount of business data to be archived [1].

5.6 Audit logs – A system of audit logs needs to be created and maintained to ensure integrity, accountability and non-repudiation while discouraging malicious activity [7].

5.7 Infrastructure – There is a need to ensure that the hardware infrastructure is of sufficient capability and capacity. Flexible, scaleable, and with redundancy in-built to cope with expanding data size and traffic loads of company growth in order to avoid “Technical Debt” [1,6].

5.8 Security training – Procedures contained within the On-boarding, Off-boarding policy should be followed with all current staff to receive training to get them up to speed [1]. Strong, unique passwords of sufficient length must be used as outlined in the password policy and multi-factor authentication enabled where possible. The practices of Job rotation and separation of duties which provide accountability must be followed as set out in the Access Control Policy [5].

5.9 Maintenance contracts – There is a need to tender for maintenance contracts for critical systems such as firewall and servers to limit file corruption due to hardware and software failures [1].

5.10 Email – System administration need to set up a corporate digital signature so staff can easily identify emails from external sources and exercise appropriate caution for phishing resulting in a breach [6].

5.11 Personal usage of Regional Gardens Ltd. data is strictly prohibited under any circumstances.

5.12 Insurance – To reduce the cost associated with the impact of potential data breaches which result in a host of problems: legal fees, interruption of business, public relations issues and possibly third party liability [1], it is highly recommended that Management procure an Cyber-Insurance policy with an appropriate level of cover.

6. Exemptions

This policy does not cover any of the following:

Data or records kept in print form.

7. Policy Review

Due to the ever changing technologies involved, this policy will be reviewed after three months to assess its effectiveness, then annually from that date unless deemed necessary to review more frequently.

Glossary

I couldn’t write this without direct quotes or plagiarism.

References

[1] Selby, N & Vescent, H. “Cyber Security and Your Business” in “The Cyber Attack Survival Manual” Weldon Owen Inc. ISBN-13: 978-1-68188-175-1, 2017. Pp 105-115.

[2] Easttom, C. “Computer security fundamentals” Upper Saddle River, New Jersey, Pearson Education Inc., 2006. Pp 145-146, 150 – 154.

[3] Schneier, B. “Secrets & Lies: Digital Security in a Networked World” Indianapolis, Indiana, Wiley Publishing, Inc., 2004. pp 68-77, 94.

[4] Pfleeger, C.P. & Pfleeger, S.L. “Security in Computing: Fourth Edition” Upper Saddle River, New Jersey, Pearson Education Inc. 2007. pp 265, 318-371.

[5] Prowse, D.L., “CompTIA Security+ SYO-501 Cert Guide: Fourth Edition” Indianapolis, Indiana. Pearson Education Inc. 2018. pp 361-384, 547-571.

[6] Stallings, W. “Cryptography and Network Security: Principles and Practices” Edinburgh Gate, Harlow, Essex. Pearson Education Limited, 2017. pp 33-37, 542-543.

[7] Whitman, M.E. & Mattord, H.J., “Management of Information Security: Sixth Edition” Boston, MA Cenage Learning, Inc. 2019. Pp 9, 169-213, 326.

[8] Shostack, A. “Threat Modeling: Designing for Security” Indianapolis, Indiana John Wiley & Sons, Inc. 2014. pp 148-153 [online] Retrieved from humblebundle.com.

[9] Pace, C. “Ch 7. Threat Intelligence for Fraud Prevention” in “The Threat Intelligence Handbook” Annapolis, MD CyberEdge Group, LLC, 2018. Pp 64-65.

[10] Australian Signals Directorate. “Essential Eight Explained”, 2019. [online] retrieved from https://www.cyber.gov.au/sites/default/files/2020-01/PROTECT%20-%20Essential%20Eight%20Explained%20%28April%202019%29.pdf

[11] Australian Signals Directorate. “Australian Government Information Security Manual”, 2020. [online] retrieved from https://www.cyber.gov.au/sites/default/files/2020-01/Australian%20Government%20Information%20Security%20Manual%20%28January%202020%29.pdf

[12] Australian Small Business and Family Enterprise Ombudsman, “The Small Business Cyber Security Best Practice Guide”, 2018. [online] Retrieved from https://www.asbfeo.gov.au/sites/default/files/documents/ASBFEO-cyber-security-guide.pdf

[13] Staman, E.M. “Policies and Practices for Ensuring Data Integrity”, 1987.

https://doi-org.ezproxy.csu.edu.au/10.1002/ir.37019875510 [online] retrieved from Wiley Online Library onlinelibrary-wiley-com

[14] Byun, J., Sohn, Y. & Bertino, E. “Systematic control and management of data integrity” [SACMAT '06: Proceedings of the eleventh ACM symposium on Access control models and technologies](https://dl-acm-org.ezproxy.csu.edu.au/doi/proceedings/10.1145/1133058) June 2006. pp 101–110 https://doi.org/10.1145/1133058.1133074 [online] retrieved from ACM Digital Library dl-acm-org

[15] Albalawi, T., Melton, A. & Rothstein, M. “A New Approach to Data Dynamic Integrity Control” [I](https://dl-acm-org.ezproxy.csu.edu.au/doi/proceedings/10.1145/2896387)CC '16: Proceedings of the International Conference on Internet of things and Cloud Computing March 2016 Article No.: 9 pp 1–8 https://doi.org/10.1145/2896387.2896394 [online] retrieved from ACM Digital Library dl-acm-org

[16] Irvine, C.E. & Levin, T. 2002. “A Cautionary Note Regarding the Data Integrity Capacity of Certain Secure Systems” pp 3-25, Gertz, M., Guldentops, E. & Strous, L. Integrity, Internal Control and Security in Information Systems: Connecting governance and technologies. [online] retrieved from Springer Link link-springer.com

[17] McBride, T., Ekstrom, M. Lusty, L., Sexton, J. & Townsend, A. 2017. “Data Integrity NIST SP 1800-11 Practice Guide” [online] retrieved from https://www.nccoe.nist.gov/sites/default/files/library/sp1800/di-nist-sp1800-11-draft.pdf