**Business Continuity Plan - Regional Gardens Ltd**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Plan Owner and Title | Phone | Email | Date | Signature |
| Chief Information Officer | 123456789 | cio@regionalgardens.com.au | 02/02/2020 |  |
| Approved By |  |  | Date | Signature |
| Executive |  |  | 02/02/2020 | Someone’s Signature |

# **Revision History**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Version | Description | Policy # | Revision Date | Review  Date | Reviewer/  Approver Name |
| 1.0 | Initial Version |  | 02/02/2020 |  | Someone elses Signature |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# **Compliance & Reporting**

|  |  |
| --- | --- |
| Compliance | Description |
| PCI DSS | Provides organizations that accept, store or transmit credit card data with guidelines for privilege management and a framework to protect cardholder data. <https://www.pcisecuritystandards.org/documents/PCI_SSC_PFI_Guidance.pdf> [1] |
| ReportCyber | Australian Cybersecurity Centre. For reporting cyber incidents and threats Australia-wide: for Individuals, Sole Traders and Small Business. <https://www.cyber.gov.au/report> [2] |
| NIST SP 800-53 | The National Institute of Standards and Technology (NIST) outlines steps in NIST SP 800-53 including reporting requirements,a standard set of data elements that must be included in any incident report. <https://www.us-cert.gov/incident-notification-guidelines-2015> [3] |
| NIST SP 800-61 | The Computer Security Incident Handling Guide. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf> [4] |

**Executive Overview**

To maintain Regional Gardens reputation, the trust of our customers, employees, and meet the associated regulatory requirements, it is essential that we do everything possible to protect the companies and customers data and resources in the face of any future Cyber related incidents. This document does not cover any physical incidents such as fire, flood, earthquakes. The more we are prepared to, the stronger our contingency planning, the faster we can respond to a potential incident, eradicate any threat, recover critical functionality and reduce the impact on our business.

The goal of this Business Continuity plan is to prepare Regional Gardens Ltdto respond in a timely, effective manner to quell the impact of any Cyber related incidents while maintaining business continuity. It defines the critical business functions, prioritises protecting the critical functionality of systems such as our Nursery Online and Onsite sales, Regional Garden Planners consultancy, corporate servers and network, which were discovered through the previously undertaken risk assessment matrix. This BCP will explore potential impacts, and contain details for response to critical incidents, while detailing strategies and actions to be taken including backup procedures disaster recovery and incident response, to enable Regional Gardens Ltd to conduct business as usual.

This plan will be updated annuallyto reflect our fresh cultural shift in towards a solid cyber security strategy and meeting or exceeding industry standards and achieving regulatory compliance. We will conduct regular testing of this plan to ensure everyone is fully trained to participate in effective incident response, backups and disaster recovery.

**Business Impact Analysis**

***Overview***

This Business Impact Analysis (BIA) is developed as part of the contingency planning process for the Regional Gardens Ltd*.* It was prepared on 02 February 2020. Template sourced and modified with permission from NIST SP 800-34 [5].

***Purpose***

The purpose of the BIA is to identify and prioritise business system assets and processes and outline the potential impact if these functions are unavailable.

The BIA is composed of the following three steps:

* **Determine business processes and recovery criticality.** Business processes supported by the system are identified and the impact of a system disruption to those processes is determined along with outage impacts and estimated downtime.
* **Identify resource requirements.** Realistic recovery efforts require a thorough evaluation of the resources required to resume business processes as quickly as possible.
* **Identify recovery priorities for system resources.** Based upon the results from the previous steps, the criticality of system resources can more clearly be linked business processes. Priority levels can be established for sequencing recovery activities and resources.

This document will be used to support the development of other contingency plans associated with the system, including, but not limited to, the Incident Response Plan (IRP), Backup Policy and Disaster Recovery Plan (DRP).

***System Description***

A small data centre is located at the companies main site comprised of:

2 Active Directory domain controllers, for authentication and authorisation

3 SQL database servers, for storing various data sets

1 Exchange Server, for email

4 File and Print Servers, for data storage and print management

2 Servers running Apache & Tomcat, for web applications and websites

3 Macbooks

and approximately 65 workstations

Internet connectivity provided by 1 ADSL connection

***Process and System Criticality***

|  |  |
| --- | --- |
| **Rank** | **Critical Business Processes** |
| 1 | Online Nursery Sales |
| 2 | In-Store Nursery Sales |
| 3 | Regional Gardens Planners |
| 4 | Customer Email & Communications |

|  |  |
| --- | --- |
| Business Process | Online Nursery Sales |
| Description | Provide customers with an online portal which they can use to purchase product at their convenience. |
| Potential Loss | Loss of online sales, loss of public image, unable to process orders inbound or outbound |
| Assets for Continuity | Internet Connection, Network, RedHat 5 Apache & Tomcat Servers, Inventory Databases, Customer Data |
| Recovery | Backups, Secondary Internet Connection |

|  |  |
| --- | --- |
| Business Process | In-Store Nursery Sales |
| Description | Provide customers with a physical shop they can use to purchase product on premises. |
| Potential Loss | Loss of in-store sales, loss of public image, unable to process orders inbound or outbound |
| Assets for Continuity | Internet Connection, Network, POS terminals, Inventory Databases, Customer Data |
| Recovery | Backups, Secondary Internet Connection |

|  |  |
| --- | --- |
| Business Process | Regional Gardens Planners |
| Description | Provide customers with garden designs, advice and consultancy services |
| Potential Loss | Loss of sales, loss of public image |
| Assets for Continuity | Internet Connection, Network, Customer Garden Project Directories, Customer Data, Workstations |
| Recovery | Backups, Secondary Internet Connection |

|  |  |
| --- | --- |
| Business Process | Customer Email & Communications |
| Description | Provide customers with online support, keep customers updated on open garden events, special sales. |
| Potential Loss | Loss of sales, loss of public image due to null response. |
| Assets for Continuity | Internet Connection, Network, Exchange Email Server, Workstations |
| Recovery | Backups, Secondary Internet Connection |

***Recovery Priorities for System Resources***

|  |  |
| --- | --- |
| **Rank** | **Critical Business Resources** |
| 1 | Internet Connection |
| 2 | Network |
| 3 | Backups |
| 4 | Active Directory Servers |
| 5 | POS Terminals |
| 6 | SQL Database Servers |
| 7 | Apache & Tomcat Servers |
| 8 | Exchange Email Server |
| 9 | File & Print Servers |
| 10 | Workstations |

***Estimated Downtime***

* **Recovery Time Objective (RTO).** RTO defines the time needed to bring critical systems back online from the point of the incident or event occurring. The Board has set an RTO of 2 hours.
* **Recovery Point Objective (RPO)**. The RPO represents the amount of time, between the last verified backup process and an incident causing disruption or data loss. The Board has set an RPO of 4 hours.
* **Work Recovery Time (WRT).** The length of time from the recovery of critical systems (RTO), through the data recovery and testing and validation processes to complete recovery.
* **Maximum Tolerable Downtime (MTD).**  The MTD represents the total amount of time from the starting point of the incident through system recovery, data recovery and testing and validation procedures to the final point of returning to normal business operation.

Estimating that the current data volume is around 3 Tb which equates to a WRT of 10hrs [6], this figure will be adjusted after accurate measurement of the volume of data sets stored by the company. but currently allowing MTD to be calculated at 14hrs. WRT ?, MTD = RTO + WRT. The systems administration team need to perform a test Disaster Recovery using the current systems to accurately measure the current WRT.

**Incident Response Plan**

***Purpose and objectives***

This plan is designed to facilitate timely and efficient response to a cyber related event or incident.

***Scope of the policy***

Effective incident response involves every department of Regional Gardens Ltd. It is important that you read and understand your role as well as the ways you will communicate and coordinate with other departments and stakeholders.

A cyber security incident comprises any accidental or deliberate event that negatively impacts the confidentiality, integrity or availability of business systems, related processes and data or customer data.

In the event of a cyber related incident, communication will be facilitated via managed alert system sending both email and SMS (Short Message Service). This will need to periodically checked to validate that this is working.

**Immediate Response & Communication Checklist** from Queensland Government Business Continuity Plan Template [7]

|  |  |  |
| --- | --- | --- |
| **Incident Response** | **** | **Actions Taken** |
| Have you:   * assessed the severity of the incident? |  |  |
| * started an Event Log? |  |  |
| * activated staff members and resources? |  |  |
| * briefed team members on incident? |  |  |
| * identified any damage? |  |  |
| * identified critical activities that have been disrupted? |  |  |
| * contacted key stakeholders? |  |  |
| * understood and complied with any regulatory/compliance requirements? |  |  |
| * initiated media/public relations response? |  |  |

**Table 3-5. Incident Handling Checklist** from NIST SP 800-61 [4]

|  |  |
| --- | --- |
| **Action** | **Completed** |
| Detection and Analysis | |
| 1. Determine whether an incident has occurred |  |
| 1.1 Analyze the precursors and indicators |  |
| 1.2 Look for correlating information |  |
| 1.3 Perform research (e.g., search engines, knowledge base) |  |
| 1.4 As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence |  |
| 2. Prioritise handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.) |  |
| 3. Report the incident to the appropriate internal personnel and external organisations |  |
| Containment, Eradication, and Recovery | |
| 4. Acquire, preserve, secure, and document evidence |  |
| 5. Contain the incident |  |
| 6. Eradicate the incident |  |
| 6.1 Identify and mitigate all vulnerabilities that were exploited |  |
| 6.2 Remove malware, inappropriate materials, and other components |  |
| 6.3 If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them |  |
| 7. Recover from the incident |  |
| 7.1 Return affected systems to an operationally ready state |  |
| 7.2 Confirm that the affected systems are functioning normally |  |
| 7.3 If necessary, implement additional monitoring to look for future related activity |  |
| Post-Incident Activity |  |
| 8. Create a follow-up report |  |
| 9. Hold a lessons learned meeting mandatory for major incidents |  |

**Roles, Responsibilities & Contact Information**

|  |  |  |
| --- | --- | --- |
| **Role** | **Responsibility** | **Contact Details** |
| **Information Security** | | |
| Chief Information Officer (CIO) | Strategic lead. Develops technical, operational, and financial risk ranking criteria used to prioritise incident response plan.  Authorises when and how incident details are reported.  Main point of contact for executive team and Board. | Name:  Phone:  Email: |
| Incident Response Team Leader and Team Members | Central team that authorises and coordinates incident response across multiple teams and functions through all stages of a cyber incident.  Maintains incident response plan, documentation, and catalogue of incidents.  Responsible for identifying, confirming and evaluating extent of incidents.  Conducts random security checks to ensure readiness to respond to a cyber attack. | * CIO * Security Manager * Systems Administrator Lead * Legal Counsel * Public Relations Liaison |
| Security Team Manager (Currently System Administration Team Leader) | Responsible for privilege management, enterprise password protection and role-based access control.  Conducts random checks to audit privileged accounts, validate whether they are required, and re-authenticate those that are.  Proactively checks for indicators of compromise.  Informs incident response team of potential attacks that compromise privileged accounts, validates and reports on the extent of attacks.  Takes action to prevent the spread of a breach by updating privileges. | Name:  Phone:  Email: |
| Systems Administration Team | Manages access to systems and applications for internal staff.  Centrally manages patches, hardware and software updates, and other system upgrades to prevent and contain a cyber attack.  Perform backups as outlined in the backup policy. | Name:  Phone:  Email:  Team Members: |
| Management | Sign off on policy changes, have the final say. | Name:  Phone:  Email: |
| Nursery Staff Team Leader |  | Name:  Phone:  Email: |
| Administration Team Leader |  | Name:  Phone:  Email: |
| Regional Gardens Planning Team Leader |  | Name:  Phone:  Email: |
| Finance Team Leader |  | Name:  Phone:  Email: |
| Human Resources |  | Name:  Phone:  Email: |
| Technical Partners (Internet Service Provider, Managed Service Providers, Hosting, Testing Partners, etc.) | Manages security controls to limit progression of a cyber attack across third-party systems and organisations. | Name:  Phone:  Email: |
| Consultants | Any Consultants who’s services are retained for expertise outside the companies current technical capabilities including Digital Forensics | Name:  Phone:  Email: |
| **Compliance & Reporting** | | |
| Legal Counsel | Confirms requirements for informing employees, customers, and the public about cyber incidents.  Responsible for checking in with local law enforcement.  Ensures IT team has legal authority for privilege account monitoring.  Communicates with regulatory bodies, following mandated reporting requirements. | Name:  Phone:  Email: |
| Insurance | Key contact person for any currently active insurance policies including Cyber. | Name:  Phone:  Email: |
| ReportCyber Australian Cyber Security Centre | Receives information about an incident according to timeline and format mandated by regulatory requirements. | Name:  Phone:  Email:  <https://www.cyber.gov.au/report> |
| PCI DSS (Payment Card Industry Data Security Standard) | Receives information about an incident according to timeline and format mandated by regulatory requirements. | Name:  Phone:  Email:  [https://www.pcisecuritystandards.org](https://www.pcisecuritystandards.org/documents/PCI_SSC_PFI_Guidance.pdf) |
| **Communications** | | |
| Marketing & Public Relations Lead | Communicates externally with customers, partners and the media.  Coordinates all communications and request for interviews with internal subject matter experts and security team.  Maintains draft crisis communications plans and statements which can be customised and distributed quickly in case of a breach. | Name:  Phone:  Email: |
| Web & Social Media Lead | Posts information on the company website, email, and social media channels regarding the breach, including our response and recommendations for users.  Sets up monitoring across social media channels to ensure we receive any feedback or questions sent by customers through social media. | Name:  Phone:  Email: |
| External Partner Companies |  | Name:  Phone:  Email: |

|  |  |  |  |
| --- | --- | --- | --- |
| **Event Log** | | | |
| Critical Event or Incident | Information | Decisions Made | Actions Taken |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Backup Policy**

To ensure the integrity of Regional Gardens Ltd Data there needs to be a strong policy on backup procedures. This document will also provide an outline to bring any new System Administrators up to speed on procedures. Some key things metrics that are missing which are needed include accurate inventory of data set volumes, the amount of time it actually takes to both backup and recover the various data sets, the physical volumes of available hard disk sizes. How can you protect what you aren’t even aware you have, so the company needs a precise inventory.

System administrators and off-site backup outsourced vendors will have access to the backups and their contact details are listed above in the Roles, Responsibilities and Contact Table. The three System administrator staff are responsible for performing the all backups. One responsible for initiating the backup process another for checking that the backups complete successfully and integrity and viability is maintained. It would be ideal if this process could be fully automated, but with the possibility of manual backup should it not initiate automatically.

To satisfy the boards requirements of a Recovery Point Objective of 4 hours, meaning the maximum sustainable data-loss based on the data needs and backup schedules. The data will be backed up with daily differential backups keeping a minimum of last two weeks of these backups, and weekly with a complete backup keeping a minimum of one months previous backups.

Following the 3-2-1 rule [8] Recommend Shadow copy of the data on a purpose-built locally based server using Raid 5, for fault tolerance [9], a tape backup also locally based and an off-site backup to be kept at an outsourced cloud based backup or data centre to be updated weekly at minimum. A Service Level Agreement (SLA) will be needed with the outsourced provider to ensure confidentiality, availability and integrity of the data while meeting or exceeding the boards Recovery Point and Recovery Time Objectives. This will give good redundancy with multiple locations and different media types should it be necessary to facilitate a recovery. The backups will need to be tested to ensure that they can be fully restored in the event of recovery.

**Disaster Recovery Plan**

***Purpose***

This plan is to facilitate the r[ecovery](http://www.business.qld.gov.au/business/running/risk-management/developing-recovery-plan) of critical business systems, processes and data to the stable state that existed prior to the cyber related incident. It will identify the required resources for the recovery process to be successful.

***Scope***

**References**

[1] PCI Security Standards Council “Payment Card Industry Data Security Standard: Requirements and Security Assessment Procedures V 3.2.1. (May 2018)” [Online] retrieved from <https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf> 02 February, 2020.

[2] Australian Signals Directorate. “ReportCyber” [Online] retrieved from Australian Cyber Security Centre <https://www.cyber.gov.au/report> 02 February, 2020.

[3] National Institute of Standards and Technology. “NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organisations” [Online] retrieved from <https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf> 02 February, 2020.

[4] Cichonski, P., Millar, T., Grance, T. & Scarfone, K. “NIST Special Publication 800-61: Computer Security Incident Handling Guide” [Online] retrieved from <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf> 02 February, 2020.

[5] Swanson, M., Bowen, P., Phillips, A. W., Gallup, D. & Lynes, D. “NIST Special Publication 800-34 Rev 1.: Contingency Planning Guide for Federal Information Systems” [Online] retrieved from <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf> 02 February, 2020.

[6] datto “Recovery Time & Downtime Cost Calculator” [Online] retrieved from <https://www.datto.com/rto/> 02 February, 2020.

[7] Queensland Government. “Business Continuity Planning Template” [Online] retrieved from https://www.publications.qld.gov.au/dataset/business-continuity-planning-template/resource/63f7d2dc-0f40-4abb-b75f-7e6acfeae8f3 02 February, 2020

[8] White, P. “Topic 10 Contingency Planning” in “ITC596 IT Risk Management Learning Material” [Online] retrieved from Charles Sturt University [https://learn-ap-southeast-2-prod-fleet01-xythos.s3-ap-southeast-2.amazonaws.com/5c1c4db3261aa/4910931?response-content-disposition=inline%3B%20filename%2A%3DUTF-8%27%27ITC596\_10\_ContingencyPlanning.pdf&response-content-type=application%2Fpdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Date=20200202T072645Z&X-Amz-SignedHeaders=host&X-Amz-Expires=21600&X-Amz-Credential=AKIAIW5OVFIUOTV36DNA%2F20200202%2Fap-southeast-2%2Fs3%2Faws4\_request&X-Amz-Signature=0bfea8cb76fb83c7d51e44038dbde4aefc564100020cc70cbe8ddfee8948864d](https://learn-ap-southeast-2-prod-fleet01-xythos.s3-ap-southeast-2.amazonaws.com/5c1c4db3261aa/4910931?response-content-disposition=inline%3B filename*%3DUTF-8''ITC596_10_ContingencyPlanning.pdf&response-content-type=application%2Fpdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Date=20200202T072645Z&X-Amz-SignedHeaders=host&X-Amz-Expires=21600&X-Amz-Credential=AKIAIW5OVFIUOTV36DNA%2F20200202%2Fap-southeast-2%2Fs3%2Faws4_request&X-Amz-Signature=0bfea8cb76fb83c7d51e44038dbde4aefc564100020cc70cbe8ddfee8948864d) 02 February, 2020.

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

[10] Whitman, M.E. & Mattford, H.J. “Management of Information Security: Sixth Edition” Boston, MA, Cenage Learning Inc. 2019.

[11] Pfleeger, C.P. & Pfleeger, S.L. “Security in Computing: Fourth Edition” Upper Saddle River, New Jersey, Pearson Education Inc. 2007.

[12] Business Queensland. “Conduct a business impact analysis” 2016. [Online] retrieved from <https://www.business.qld.gov.au/running-business/protecting-business/risk-management/preparing-plan/impact-analysis>

02 February, 2020.

[13] SBS CyberSecurity. “{Article} What does a good BIA look like” 2017. [Online] retrieved from <https://sbscyber.com/resources/article-what-does-a-good-bia-look-like> 02 February, 2020.

[14] Australian Signals Directorate. “Strategies to Mitigate Cyber Security Incidents (February 2017)” [Online] retrieved from [https://www.cyber.gov.au/sites/default/files/2020-01/PROTECT%20-%20Strategies%20to%20Mitigate%20Cyber%20Security%20Incidents%20%28February%202017%29\_0.pdf](https://www.cyber.gov.au/sites/default/files/2020-01/PROTECT - Strategies to Mitigate Cyber Security Incidents (February 2017)_0.pdf) 02 February, 2020.

[15] Australian Signals Directorate. “Developing an incident response plan” [Online] retrieved from <https://www.cyber.gov.au/advice/developing-an-incident-response-plan> 02 February, 2020.

[16] Crowley, C & Lee, R. “SCORE Security Checklist” in “Score Checklists & Step-by-Step Guides” [Online] retrieved from SANS Institute <https://www.sans.org/media/score/checklists/APT-IncidentHandling-Checklist.pdf> 02 February, 2020.

[17] Kral, P. “Incident Handler’s Handbook” 2011. [Online] retrieved from SANS Institute <https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901> 02 February, 2020.

[18] Chaitow, J. “There’s a hole in my infrastructure? The road to PCI Compliance” 2019. [Online] retrieved from SANS Institute <https://www.sans.org/reading-room/whitepapers/compliance/hole-infrastructure-road-pci-compliance-32834> 02 February, 2020.