STRATEGIC BCP®

INFORMATION SECURITY MANAGEMENT and GOVERNANCE GUIDELINES

Policy Statement

This volume is intended to be an over-arching guideline to managing Information Security and outlines the framework for management of Information Security within the Company.

These Information Security Management guidelines apply to all forms of information including:

- Speech, spoken face to face, or communicated by phone or radio,
- Hard copy data printed or written on paper,
- Information stored in manual filing systems,
- Communications sent by mail, courier service, facsimile or electronic mail,
- Stored and processed via servers, PC's, laptops, mobile phones, PDA's,
- Stored on any type of removable media, CD's, DVD's, tape, USB memory sticks, digital cameras.

Maintaining the security, confidentiality, integrity, and availability of information stored in the Strategic BCP (the "Company") workstations, files, cabinets, computer networks (hosted or captive) and data and electronic communications infrastructure ("Company Systems") is a responsibility shared by all users of those systems. All users of Company Systems are responsible for protecting those resources and the information processed, stored or transmitted thereby as set forth in this policy. Violations of this policy may result in disciplinary action up to and including termination.

This policy is based upon ISO 27002 and is structured to include the main security category areas within the standard. This policy is a high level policy which is supplemented by additional security policy documents which provide detailed policies and guidelines relating to specific security controls. Specifically, in addition to this volume, please refer to additional more focused requirements appearing in the Company's Information Security Policy.

The Information Security Policy document and other items included or referenced herein set forth the Company's approach to managing information security. This policy shall be reviewed annually for sufficiency.

Purpose

Information is a vital Company asset and requires protection from unauthorized access, modification, disclosure or destruction. This policy sets forth guidelines for the management of availability and security systems within the Company.

Distribution

All employees and subcontractors. Information Security and availability standards, processes and procedures apply to all staff and employees of the organization, contractual third parties and agents of the organization who have access to the organization's information systems or information.

Table of Contents

Information Resources

The Company's Information Resources (IR) are comprised of any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer embedded technology, telecommunication resources, network environments, telephones, fax machines and printers.

IR also is comprised of the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

The Company's third party managed hosting environment is considered IR and is also subject to this management policy as well as other Company policies.

The Company's ResilienceONE software is considered IR and is subject to this policy as well as other Company policies.

Information Security Governance and Compliance

The chief objective of Information Security Management is to institute appropriate measurements in order to eliminate or minimize the impact that various security related threats and vulnerabilities might have on the Company. Users of Company Systems or data/information are responsible for protecting the information processed, stored or transmitted over or on those systems, and for incorporating the practices outlined herein into their daily activities.

The Chief Information Officer (CIO) is the designated owner of the Information Security Policies, governance and guidelines and shall review and make recommendations on the availability policy, security policy, policy standards, directives, procedures, Incident management and security and availability awareness education.

Regulatory, legislative and contractual requirements shall be incorporated into the Information Security Policy, processes and procedures. The requirements of an Information Security Policy as well as processes, and procedures will be incorporated into the Company's operational procedures and contractual arrangements.

The Company's Management team shall convene on a quarterly basis to discuss all matters related to topics covered in this and all of the Company's Policies and Procedures. These quarterly meeting shall also discuss developments in IT and changes in laws and regulations that may impact the Company's IR and the general integrity, availability and security of its software products. Any deficiencies or other issues arising as a result of these meeting shall be discussed and placed on a standing agenda to be addressed for remediation.

Risks

Data and information which is collected, analyzed, stored, communicated and reported upon may be subject to theft, misuse, loss and corruption. Data and information may be put at risk by poor education and training, misuse, and the breach of security controls. Information security incidents can give rise to embarrassment, financial loss, non-compliance with standards and regulations as well as possible judgments being made against the Company.

The Company shall and does undertake risk assessments to identify, quantify, and prioritize risks and controls will be selected and implemented to mitigate the risks identified. Additionally, periodic risk assessments shall be and are undertaken using a systematic approach to identify and estimate the magnitude of the risks. Further, the Company's ResilienceONE software is utilized internally to pinpoint enterprise and operational risks and to track their successful remediation.

Organization and Development

It is the policy of the Company to ensure that information will be protected from a loss of:

- Confidentiality: so that information is accessible only to authorized individuals.
- Integrity: safeguarding the accuracy and completeness of information and processing methods.
- Availability: that authorized users have access to relevant information when required.

The Company intends that its procedures are organized to work towards implementing the ISO 27000 standards. Guidance shall be provided on what constitutes an Information Security Incident. All breaches of information security, actual or suspected, must be reported and will be investigated. Business continuity plans shall be produced, maintained and tested in the Company's resident instance of ResilienceONE® software. Information security and availability education and training will be made available to all staff and employees. Information stored by the Company will be appropriate to the business requirements.

The security and availability of information will be managed within an approved framework through assigning roles and co-ordinating implementation of this security policy across the Company and in its dealings with third parties. External advice will be drawn upon where necessary so as to maintain the Information Security Policy, processes and procedures to address new and emerging threats and standards.

- The CIO is the designated owner of the Information Security Policies and is responsible for the maintenance and review of Information Security Policies, processes and procedures.
- Department heads are responsible for ensuring that all staff and employees, contractual third parties and agents of the Company are made aware of and comply with Information Security Policies, processes and procedures.
- The Company's auditors shall review the adequacy of the controls that are implemented to protect the Company's information and recommend improvements where deficiencies are found.
- All staff and employees of the Company, outside contractors and agents accessing the Company's information are required to adhere to the Information Security Policies, processes and procedures.

Failure to comply with Information Security Policies, processes and procedures can lead to disciplinary or remedial action.

The Information Security Policy shall have been approved by management and communicated to all staff and employees of the Company, contractual third parties and agents of the Company. The security requirements for the Company shall be reviewed at least annually by the CTO and CIO, and other senior staff, as necessary, and approved by the President and Board of Directors.

Formal requests for changes to this and any Information Security Policy shall be addressed either to the CIO or CTO and/or President of the Company.

Asset Management and Security Practices

The Company is committed to adequately and appropriately protecting its assets and property. All assets (data, information, software, computer and communications equipment, service utilities, and licenses and other intellectual property) whether leased or owned shall be accounted for and have an owner or overseer.

Owners or overseers shall be identified for all assets and intellectual property and they shall be responsible for the oversight, maintenance and protection of their respective assets.

Awareness and Training: The Company's security policies shall be communicated to all employees, contractors and third parties to ensure that they understand their responsibilities. It is the Company's policy to annually conduct security awareness training for asset management. Such training shall include but not be limited to:

- The nature of Company assets and operations such as trade secrets and privacy.
- Employee and contractor responsibilities in handling assets and sensitive information.
- Requirements for proper handling of sensitive material in physical form, including marking, transmission, storage and destruction.
- Proper methods for protecting sensitive information on computer systems, including password policy.
- Workplace security, including physical access and reporting of incidents.
- Consequences of failure to properly protect assets.

Communications: It is the Company's policy that all written and spoken communications dealing with confidential or sensitive subject matter be handled in a secure fashion. Conferences, meetings and discussions where sensitive and confidential information is communicated shall be conducted at facilities (or in such manner) that insure the privacy of the communications.

Physical Environments: Critical or sensitive information processing facilities (whether internal or external including managed hosting) shall be housed in secure areas and shall be operated in a safe and secure manner. The secure areas shall be protected by defined security perimeters with appropriate security barriers and entry controls. Critical and sensitive information shall be physically protected from unauthorized access, damage and interference. Outside managed hosting providers shall be SSAE-16/SAS-70 certified (or applicable equivalent certification).

Managed Hosting Oversight: The Chief Operations Officer, together with the Chief Technical Officer, shall jointly be responsible for the management, operation and ongoing security and availability of all data and information processing functions at the Company's managed hosting facilities. The Company shall only use managed hosting providers that are SSAE-16/SAS-70 certified (or applicable equivalent certification).

HR: Security responsibilities shall be included in job descriptions and in terms and conditions of employment. Verification (or background checks, as applicable) checks shall be carried out on all new employees, contractors and third parties. Segregation of duties will be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse.

Accessibility and Identity

Access to all information, Company application and Company Systems (including internal and any and all cloud-based systems) shall be controlled and shall be driven by business requirements. Access will be granted or arrangements made for employees, partners, suppliers according to their role, only to a level that will allow them to carry out their duties. See also the Company's Application and Systems Access Policy.

For use of the Company's Resilience ONE software , a user registration (and de-registration) is required to gain access to either 1) any instance of the software or 2) any instance of the software code. In either case, employees or contractors who have left the employ of the Company shall be prohibited from access immediately upon separation. The Chief Technical Officer shall be responsible for oversight of these processes.

For use of the Company's e-mail systems, user registration (and de-registration) is required to establish an e-mail account. Employees who have left the employ of the Company shall be prohibited from e-Mail access immediately upon separation. The Chief Technical Officer shall also be responsible for oversight of these processes.

Use of the Company's website shall be governed by separate privacy and terms of use policies. The Company's website shall strive to be EU Safe Harbor and Swiss compliant.

A separate Information Security Policy outlines protocols for workstation management, clean desk and password construction to assure safe and secure access and use.

Security and Availability

The Company assures its clients (through its Service Level Outline) a certain degree of availability and security of its software products. One element of this assurance is the promised integrity of its third-party hosting provider which integrity is presumed fulfilled through the Company's resolve that such third-party provider be SSAE-16 compliant. While the Company believes that said integrity is achieved by such compliance, it also believes that it needs to periodically monitor and test this compliance as relates to the Company's hosted software product.

Accordingly, the Company shall monitor its outsourced hosting provider for the integrity and performance of those functions that are outsourced. Specifically, this monitoring shall include (but not be limited to) the following functional elements:

- Antivirus
- Firewall
- Server Performance
- Backup Integrity
- Backup Restoration

Security and availability reviews and vulnerability assessments of outsourced functions shall be performed by Company IT personnel or third-party vendors, as may be necessary. Such assessments shall be reviewed at the quarterly Management meetings where known or anticipated issues shall be scheduled for remediation and added to the team's standing remediation agenda.

Additionally, the Company shall insure that backups conducted by its third-party hosting provider are of sufficient availability and integrity. This shall be accomplished by annual testing of backup restoration of a random data source. The ability to recall backup media located at third-party providers shall be restricted to the Company's President, CTO and CIO, or a suitable designee as approved solely by the President.

The CTO, CSO and CIO shall collectively be responsible for oversight of the processes relating to Security and Availability.

Vulnerability Management

The Company's Vulnerability Management policy appears under separate cover and elsewhere among the Company policies and procedures.

Change Management

The Company views Change Management as a systematic approach to dealing with change, both from the perspective of an organization and on the individual level. Change management has at least three different aspects, including: adapting to change, controlling change, and effecting change. A proactive approach to dealing with change is at the core of the Company's approach to Change Management. The Company views Change Management as the means of defining and implementing procedures and/or technologies to deal with changes in the business environment and to profit from changing opportunities. Information security requirements and availability protocols will be defined during the development of business requirements for new information systems or changes to existing information systems.

The Company’s Change Management policy appears under separate cover and elsewhere among the Company policies and procedures.

Escalation Management

There are two basic distinctions within the Company’s Information Resources (IR) – IR that is internal to the Company (used on Company equipment) and IR that is hosted off-site. The key component of the Company’s Information resources (IR) is its ResilienceONE software that is hosted and maintained off-site.

Managed Hosting System

Instances of the Company’s software application, ResilienceONE, are maintained in an outside, third-party, environment. The application is a SaaS application and is currently maintained at facilities overseen and owned by Rackspace Hosting, Inc. Currently, instances of the software are primary in Grapevine, TX with failover at Ashburn, Virginia. Instances at Ashburn are mirrored from Grapevine. The following is an outline of current escalation protocols in place.

Rackspace Escalation:

Account Manager → Team Lead Director → Vice President of Customer Care

Rackspace data center engineers or support technicians respond to alerts generated from the various forms of monitoring procedures[1]. The Rackspace customer care team utilizes a Rackspace tool called CORE to manage services to customers. The CORE ticketing system was specifically developed by Rackspace as a support tool for the managed hosting industry. CORE stores relevant information about a customer and associated servers and services. CORE is also used to track customer trouble tickets, or incidents. Automated problem escalation procedures are in place to ensure that CORE trouble tickets are escalated if unresolved.

Rackspace personnel use its ticketing system to document and track incidents and communicate with customers. CORE tickets generate email alerts directly to customers when they are created or updated. Utilizing built-in rules, tickets are routed to the appropriate team(s) for automated escalation. CORE is utilized to track communication between the customer and Rackspace via a ticket with the following minimum fields captured: date/time stamping, ticket category, customer number, data center location and device location. All the modifications, including who made them and when, provide the customer and Rackspace with an audit trail of the current and past issues and their resolution, viewable by the customer through the MyRackspace customer portal. Escalation procedures are in place and communicated to Strategic BCP so that it has access to Rackspace management for discussion, resolution and post-incident review.

Rackspace will continuously monitor all servers to detect any availability and/or security incidents or anomalies. Upon detection Rackspace immediately notifies the contacts at Strategic BCP.

[1] The Microsoft Operations Manager (MOM) monitoring tool is used to monitor various Microsoft services on all Intensive and RES customers’ hosting environments including:

● Windows 2003/2008
● Terminal Services
● Active Directory
● Internet Information Services (IIS)
● SQL Server

Metrics collected by MOM are used to provide performance and storage capacity reporting. MOM is used to administer Windows servers, utilizing tools to track performance and address tasks such as database and operating system level events. MOM helps simplify identification of issues and streamlines the process for determining the root cause of the problem. It also facilitates quick resolution to restore services and serves to prevent potential problems to Rackspace’s customers.

Rackspace also provides a Linux monitoring tool, which is utilized for all Intensive Linux customers, unless they opted out of the service. The tool is used to monitor various Linux services on Intensive’s Linux customer environment including :

● CPU, DISK, MEMORY (CDM)
● Hardware Failure (Dell servers)
● Running processes
● Oracle Databases
● Log files

Strategic BCP (SBCP) Escalation:

Technical Operations Director → CTO → COO → President

SBCP is informed of scheduled downtime and emergency changes on a timely basis via the ticketing system or via customer portal e-mail. SBCP will interact with the Rackspace ticketing system in real-time through its company portal. SBCP's portal will contain reports on data from several monitoring tools, and is a separate data repository on a segregated environment from the software production environment.

SBCP personnel would immediately contact Client personnel of any impact that may affect ResilienceONE operation. Problem resolution will also be tracked in the ResilienceONE online ticketing system. SBCP would create a ticket in its own ticketing system and periodically update so that Client personnel can track the remediation progress. Once corrected, a "post-incident" assessment would be performed to identify the elements of the availability and/or security issue breached (if any) or the elements of the occurrence that caused the availability and/or security issue to provide a roadmap for mitigating impacts.

Internal Systems and Software Management

Internal Systems

The Company does not lease, own or maintain any servers at its facilities. Additionally, the Company does not have any Cloud facilities other than those related to ResilienceONE.

Company IT systems are workstation-based and are solely comprised of desktop or laptop computers and related peripherals. Accordingly, incidents of compromise or of failure of device applications are principally those related to their resident software applications, firmware or hardware. Incident escalation would mirror the escalation process for Managed Hosting:

Internal Systems SBCP Escalation:

Technical Operations Director ⇨ CTO ⇨ COO ⇨ President

Software Issue Tickets

For issues or problems associated with Client usage of ResilienceONE software, the Company employs a ticketing system contracted from a third-party resource. – SysAid. Under separate cover, the Company has set forth a process for Client Instance Management of ResilienceONE. The following is a summary of the escalation process:

Level 1 Ticket Support ⇨ Level 2 Ticket Support (IT) ⇨ CTO ⇨ President