

Assurance Program

The GCRH Corporation and its suppliers, contractors, partners, associates, and affiliates (collectively "GCRH") use best efforts to provide state of the art security, back-up, and disaster recovery plans, procedures and equipment. The plans, procedures and equipment now in effect or in use as part of our standard assurance program are outlined below. However, GCRH reserves the right to modify, change or terminate each of the items described below at its sole discretion and without notice.

1. Standard Infrastructure Security

A. Physical Environment

- Concrete building structure designed to Seismic Zone 3 Essential Services criteria.
- Redundant fiber entry into the building with multiple Internet Service Providers.
- Diesel powered emergency generator with two-week operating capacity.
- Fire-threat detection and suppression system.
- Raised access floor with copper massive grounding system.
- Controlled temperature and humidity environment with fully redundant HVAC system.
- Biometric and card reader controlled doors at all entrances and exits.
- Locking collocation cabinets with dual 100 Mbps fast Ethernet cross connects.

B. Internet Security

- Compartmentalization – The network is laid out to provide compartmentalization between service types, between customers, and between services provided to customers. Certain subsystems are assigned private addresses that are not routable across the Internet.
- Host Hardening – Hardening means removing default items that have low value, but create a certain amount of vulnerability and compromise for the system.
Hardening a system protects it from unauthorized usage, restricts access to critical areas, and helps assure that if something happens, it doesn't cause system failure.
- 128-bit Secure Socket Layer (SSL) Encryption of Web RA Site Traffic – SSL technology protects sensitive information using both server authentication and data encryption. This encryption makes interpretation impossible for anyone other than the intended recipient. Verisign, a third party Certification Authority (CA), has verified these details.

- Application of OS and Database Patches – Vendor web sites are monitored on a daily basis to check for critical security patch releases.

2. Standard Backup Processes

A. Data Backups

- Each RightAnswer® solution implementation is backed up on a daily basis.
- Each Backup "Snapshot" contains:
 - A complete set of the scripting for the implementation;
 - All client uploaded files; and
 - A backup of the database for the given implementation.
- Snapshots are encrypted and sent to a storage array in Denver, Colorado on a daily basis.

B. Back-Up Equipment

- Spare servers are available at the data center in Seattle, Washington.
- Additional spare servers are available in a second location in Kirkland, Washington.

3. Standard Disaster Recovery Process

A. System Monitoring

- Periodic sampling of each RightAnswer® solution subsystem (6 minute intervals) by external auditor.
- Warning sent to pager of on-call technician upon any test failure.

B. Escalation Sequence

1. Technician attempts to diagnose and resolve the problem remotely.
2. Technician goes onsite to diagnose and resolve the problem, if necessary.
3. Technician implements the Disaster Recovery Process in Seattle, Washington.
4. Technician requests implementation of the Disaster Recovery Process in Midland, Michigan.

C. Disaster Recovery Process

- The most recent Snapshot of the implementation to be recovered is retrieved from the storage array.
- The Snapshot is loaded onto spare servers, as required, at the data center.
- Additional transaction logs after the Snapshot was taken, if available, are loaded onto the spare servers.
- Additional client file updates made after the Snapshot was taken, if available, are loaded onto the spare servers.

4. Standard Security Audits

A. Security Practice Objectives

- Confidentiality: Maintain data privacy and minimize the risk of unauthorized access or disclosure, internally or externally.
- Integrity: Prevent unauthorized alteration or loss of data.
- Availability: Minimize downtime and recovery delays.

B. Security Audits (are or can be performed based on Customer Requirements)

- External Unauthorized access at the Operating System (OS) – Checks that the Operating System has the appropriate patches/updates to guard against malicious unauthorized access to/through the OS. A third party has performed these services on our OSs and has been engaged to perform these audits regularly to ensure our OSs are current.
 - Audit Interval: 1 time/month (or more often as patches are released)
- External Unauthorized access (hacking) to the RightAnswer® application – This audit tests for vulnerability of the particular application/website.
 - Audit Interval: Annually
- Disabled UserID's Audit – Verifies that users cannot access the system via hacking or book marked pages.
 - Audit Interval: Annually
- Physical Security Audit – Tests the physical access to the Data Center/Servers.
 - Audit Interval: Annually
- Business Process Audit – Checks the business processes used to manage the systems/accounts.
 - Audit Interval: Annually

C. Security Audit "Checklist":

- Physical Security – Data Center Security
 - Biometric and card reader controlled doors at facility entrance/exit.
 - Security guard on-duty 24/7/365.
 - Controlled access to locking co-location cages and cabinets.
- OS Security
 - Application of OS and Database Software Patches
 - Vendor web sites monitored daily to check for critical security patch releases.
 - Log Review
 - Audit logs for changes and unusual access patterns.
 - Host Hardening
 - Remove default services that the given server doesn't require.
 - Change Default Passwords
 - Prior to connecting each new server to the Internet, change any default passwords.
- Network Security
 - Compartmentalization
 - Structure the network to provide compartmentalization between service types, between customers, and between services provided to customers. Certain subsystems are assigned private addresses that are not directly routable across the Internet.
 - Switched VLAN
 - Use VLAN services to isolate every customer, making each operation look as though it is alone in the data center. VLAN technology isolates traffic into separate LANs, as though each LAN is on a dedicated switch.
- Application Security
 - End-to-End Session Encryption
 - Independent Session ID assigned with each user session.
 - Automatic timeout of Session ID's.
 - All web pages (except the login page) require valid session ID for access.
 - 128-bit Secure Socket Layer (SSL) Encryption used for all communications.
- Mistrust of User Input
 - All user-submitted data is checked on the server-side (in addition to the client-side, if available) to make sure inputs conform to

business rules prior to processing by the application. Strings that could contain HTML or JavaScript are stripped of suspicious tags and are checked against length constraints to prevent buffer overflows.

- Safe Data Handling
 - MD5 encryption of user passwords within backend databases.
 - Removal of hard-coded passwords and backdoors from application code.
 - Segregating stored information so that customers cannot access each other's data, even in the event of a compromise.
- User Access Rights
 - User and group access rights control exactly which documents (or portions thereof) that each user is allowed to view and/or update.
- Penetration Testing
 - Simple Attack Simulation
 - This test attack will simulate the behavior and techniques of low skill set intruders or "script kiddies". Such attacks represent the majority of intruder activity on the Internet.
 - Skilled Attack Simulation
 - This simulation includes skill sets involving high-level database knowledge, knowledge of application vulnerabilities, advanced networking skills, and high-end exploitation tools.
 - Customer/Partner Attack Simulation
 - Simulates customer or partner attacks into privileged access areas. Tests the ability of the system to detect and respond to security risks associated with partner and customer deep access.
 - Insider Attack Simulation
 - Simulates a threat from skilled insiders with access from the internal network.
 - Helps test and establish detection and response methods meant to contain sources of damage from within the corporate infrastructure.

5. Standard Infrastructure:

A. Shared Servers Infrastructure

- Dedicated RightAnswer® solution Application "Instance" (copy of code)
- Dedicated RightAnswer® solution DataBase "Instance" (copy of code)
- Shared Web Server
- Shared DataBase Server
- Shared server/hardware/software environment for general system services such as rendering engine, autoID/barcode server, auto document distribution server, and other servers for general "system services".

Additional security, testing, audits, etc.

Customers may request additional security, testing, audits or related services. Upon receipt of customer specifications, GCRH will provide an estimate if requirements will incur additional charges.

GCRH offers additional infrastructure options for customers seeking a premium package. F**

1. Infrastructure Option 1 – Dedicated Direct Servers and Shared Indirect Servers: “Dedicated-Direct”
 - Dedicated RightAnswer® solution Application
 - Dedicated RightAnswer® solution DataBase
 - Dedicated Web Server
 - Dedicated DataBase Server
 - Shared server/hardware/software environment for general system services such as the rendering engine, autoID/barcode server, auto document distribution server, and other servers which provide general systems services.

2. Infrastructure Option 2 – Dedicated Direct Servers and Dedicated Indirect Servers: “Dedicated-Direct/Indirect”
 - Dedicated RightAnswer® solution Application
 - Dedicated RightAnswer® solution DataBase
 - Dedicated Web Server
 - Dedicated DataBase Server
 - Dedicated server/hardware/software environment for general system services such as the rendering engine, autoID/barcode server, auto document distribution server, and other servers as appropriate, which provide general systems services.
 - ⇒ Switched VLAN – VLAN services isolate every customer, making each operation look as though it is alone in the data center. VLAN technology isolates traffic into separate LANs, as though each LAN is on a dedicated switch.

3. Infrastructure Option 3 – Mirrored Infrastructure for Dedicated Direct Servers and Dedicated Indirect Servers: “Dedicate Direct/Indirect/Mirrored – Active/Passive”
 - Dedicated RightAnswer® solution Application
 - Dedicated RightAnswer® solution DataBase
 - Dedicated Web Server
 - Dedicated DataBase Server
 - Dedicated server/hardware/software environment for general system services such as the rendering engine, autoID/barcode server, auto document distribution server, and other servers as appropriate, which provide general systems services.
 - ⇒ Switched VLAN – VLAN services isolate every customer, making each operation look as though it is alone in the data center. VLAN technology isolates traffic into separate LANs, as though each LAN is on a dedicated switch.
 - ⇒ The above infrastructure is duplicated at a

- second location, with database transactions being immediately/simultaneously sent to the second set of servers for real-time back up.
 - ⇒ If the first set of servers fail, the second set of servers (previously “passive”) take over and become “active” to provide on-going access to users.

4. Infrastructure Option 4 – Mirrored Infrastructure for Dedicated Direct Servers and Dedicated Indirect Servers: “Dedicated-Direct/Indirect/Mirrored – Active/Active”
 - Dedicated RightAnswer® solution Application
 - Dedicated RightAnswer® solution DataBase
 - Dedicated Web Server
 - Dedicated DataBase Server
 - Dedicated server/hardware/software environment for general system services such as the rendering engine, autoID/barcode server, auto document distribution server, and other servers as appropriate, which provide general systems services.
 - ⇒ Switched VLAN – VLAN services isolate every customer, making each operation look as though it is alone in the data center. VLAN technology isolates traffic into separate LANs, as though each LAN is on a dedicated switch.
 - ⇒ The above infrastructure is duplicated at a second location, with database transactions taking place on either of the set of servers (e.g., for load balancing).
 - ⇒ Both sets of servers immediately/simultaneously transmit transactions to the other set of servers for real-time back-up.
 - ⇒ If one set of servers fails, the other set of servers is already running (e.g., “active”) thus providing seamless on-going access to users.