Information Technology Disaster Recovery Plan

On a regular basis, the IT Director shall:

1) Ensure IT employees are familiar with the Emergency Response Plan for Employees and know what to do in an emergency situation.
2) Backup critical data daily and regularly secure this information at an offsite location.
3) Maintain documentation for, and back up of, all electronic equipment, software and system configurations.
4) Keep records of all software purchases and licenses.
5) For critical subcontractors and suppliers, specify at least one of the following:
   - Insist that they have an effective emergency plan that will enable them to continue to provide services/supplies in the event of a disaster at their business.
   - Identify backup subcontractors and suppliers. (This is especially important for local providers that are also vulnerable to the same local community-wide disasters.)
   - Do business with multiple subcontractors and suppliers.
6) Maintain the IT department's Disaster Recovery Plan (DRP).
7) Develop and maintain an IT Alternate Site Plan.
8) Identify all important equipment and document the vendor(s), alternate vendor(s), estimated replacement time, and level of importance.
9) Update anti-virus software on a regular basis and maintain an Information Security Plan.

When Alerted of an Impending Disaster, the IT Director shall:
(to the extent that time permits and as instructed by the ERT)

1) Be prepared to execute the Disaster Recovery Plan.
2) Be prepared to activate the IT Alternate Site Plan.
3) Perform a special backup of all systems; secure backup disks offsite.
4) Secure work area during a warning.
5) Inform all users of a pending system shutdown.
6) If necessary, shutdown all systems.
7) If necessary, implement appropriate evacuation, shelter-in-place and safety plans.

When a disaster has impacted the ICVB, the IT Director shall:

1) Discontinue all normal business activities.
2) If necessary and if time permits, shutdown all systems.
3) Implement appropriate evacuation, shelter-in-place and safety plans.

Post-Disaster Activities (depending upon the level of damage and as instructed by the ERT)

Response

1) Do not turn on electrical equipment if corrosive contaminants are present or if the power supply is unreliable.
2) If applicable, disconnect all electrical equipment. As a safety precaution, first disconnect electrical power at the main circuit breaker.
3) Contact telecommunication providers.
4) Assess damages, identify destroyed & salvageable equipment, and send assessment to the ERT.
    - Computers
    - File Servers
    - Telecommunication Equipment
    - Peripheral Equipment
    - Data
    - Other
5) Be prepared to implement the Disaster Recovery Plan.
6) Be prepared to activate the IT Alternate Site Plan.
7) Order replacement equipment if the disaster is clearly restricted to hardware.
8) Contact critical suppliers and vendors.

Recovery

1) Initiate the Data Center cleanup, reconstruction and/or relocation efforts.
2) Relay information regarding personnel to Administration.
3) Maintain the IT Alternate Site.
4) Contact critical subcontractors and vendors.
5) Make critical (if only temporary) repairs.
6) Repair salvageable equipment and institute the replacement of critical equipment.
7) As soon as a physical facility with reliable power and communication capability is secured, initiate the replacement of destroyed or disabled equipment.

Long Term

1) Review the Department Plan.
2) Review vendor, subcontractor and supplier performance.

Primary Recovery Responsibilities

1. Execute the Disaster Recovery Plan.
2. Execute the IT Alternate Site Plan if directed.
3. Systems support to mission-critical business services.
4. Telecommunications to mission-critical business services.
5. Assess damage to workspace & equipment.

Equipment Requirements

Department/Equipment Name	Manufacturer	Primary Function(s)	Level of Importance	Time to Replace	Alternatives	
					Manual	Outsource
6 Bureau – Servers Data, Exchange, Spot, BDR, Domain Controller, BDC-Print Server.	DELL	Server	High	This is in the process of being changed to virtual servers, which will be completed over a two-year period.	IT Director	Fulcrum Group/ Jason Denton
Phone system	DIGIUM	Phone System/ Voice Mail	High		IT Director	Fulcrum Group
10 Admin– Computers/loaners	DELL	Computers	High		IT Director	
9 Sales – Computers	DELL	Computers	High		IT Director	
9 MarCom-Computers	DELL	Computers	High		IT Director	
10 Printers-owned	HP	Printer	Low		IT Director	
7 Printers-leased	Nova Copy	Printer/Scanners	Medium			Nova Copy

Systems Requirements

Dept/App	Platform	Location	# of Users	Key Interfaces (If Any)	Business Impact (If Lost)	Recovery Time Objective	Comments / Future Status
CRM	Web Based	Web	22	Barb Schingle	High	Immediate	Web
Banner	Citrix	City	5	Marianne Lauda	High	2-5 business days	In process of moving to web
*****If the Bureau connection is lost, the recovery is fairly easy; if the City "source" is lost, then recovery is a major issue. The City would have to get up and running before the Bureau could process its activity.							
Outlook 2010-2016 on O365 licenses	Windows 2008	Bureau	23	Barb Schingle	High	Immediate through Spot Recovery 2-5 business days for full restore	Will move to O365 after Banner becomes Web Based
Microsoft Office/Word/Excel 2010-2016 on O365 licenses	Windows 7	Bureau	23	Barb Schingle	High	2-5 business days- Immediate for remote	Will move to O365 after Banner becomes Web Based
Adobe Creative Cloud and Acrobat DC	Windows 7	Bureau	22	Barb Schingle MarCom	Normal	Immediate for users with remote laptops and computers	Web

Computer System Back up Plan

The following information outlines the plan to implement network and workstation computers in the event the current office at the ICC is rendered unusable and all equipment is damaged.

Every weekday a full backup and incremental backups are done of all the data files on the servers to an offsite cloud. One laptop, the Executive Director's is also backed up to the cloud, when the computer is onsite.

In the event of a disaster to the ICC, The Fulcrum Group, our third-party support vendor can, to a degree, recover our data in the Storagecraft Public Cloud immediately after a disaster and be up and running within 48 to 96 hours. Storagecraft Public Cloud Recovery is free for 2 weeks. If all existing hardware is destroyed in a disaster, then new hardware would have to be procured, and professional services would be required to rebuild and recover the server environment. A current estimate is about $75,000 for services. Hardware replacement costs would go through the Computer Replacement Fund, which is already in place.

Each year, an emergency backup laptop (current make/model) will be configured with the current Bureau network/software and kept at an off-site location that is accessible by the Technology Director. That computer will be kept up to date monthly, and will have all the additional application software that is needed to configure any Bureau computer.

In the event of a disaster, the CVB will purchase several of same make and model of laptops with the Bureau American Express Card and The Fulcrum Group will send several technicians to help reload any new computers which have been purchased due to the disaster. It should be noted that MarCom has 4 laptops at home, Accounting has one and the Technology Director has the emergency backup laptop, enabling those people to work remote with limited access to email and access to the network drives. The Executive Director's computer is backed up daily to a remote cloud, when onsite at the office. The new laptops will be distributed to any additional employees deemed necessary, based on need and whose computers have been damaged.

VPN and Citrix software (or current remote connection software) will be installed and configured to work on the laptops. Laptops will be given to the appropriate personnel, so they can access CRM, ICVB email, internet, and server data files from a remote location. The remote location would need internet connectivity (such as a home, office, hotel with wireless internet connectivity). Currently laptops are configured to connect through wireless.

The executable files for Adobe Acrobat and Adobe Creative Cloud will be kept with the off-site laptop; hard copies of all cloud software access will also be kept at the remote location. When new computers are purchased, the Adobe software will be loaded for those who need it. As part of the disaster recovery plan, SPOT Email Security has the Business Continuity feature, where users can send/receive email from their SPOT Email Security Quarantine portal. It's not the most elegant solution in the world, but it's very inexpensive (free, included in the base SPOT Email Security service). Note, only current and future email can be accessed from this feature, not any email that was in the Inbox/Sent prior to the disaster. All email will be accessible after the email server is restored. Personal Folders and information that is kept locally on the computer is backed up every two months, so depending on when the disaster occurred, some information may be unrecoverable if it was stored locally on the machine.

The accounting department within ICVB uses application software called Banner. It is connected to City Hall via the Internet and accessed through the Intranet and Citrix. It is configured and run through City Servers at City Hall. In the event the ICC is destroyed, the accounting department could access Banner from the Arts Center, Finance Department at City Hall, or from a remote location through VPN/Citrix. The backup server for Banner is at the Police Department. In the event that City Hall was also destroyed, the server at the Police Department would be used to run the Banner Software. The accounting department could access Banner from the Irving Police North Sub-station. If both City Hall and the Police Station were destroyed, a third plan would have to be negotiated with City Hall to recover the backup tapes from their backups, have the Vendor restore the application on a server and restore the data from the cloud. This option will change in the next couple of years when a new online system is purchased, and the old system is converted to online access. At that time, ICVB will be moving to O365 online.

The Bureau would be able to use the existing licenses for O365/2016 Adobe Creative Suite and Adobe Acrobat DC, and Symantec for any equipment that needs to be purchased. All other software is on the servers and on the emergency backup laptop.

A few printers may also have to be purchased and or leased from Nova Copy depending on the set of circumstances.

Simpleview CRM Disaster Recovery Plan

Technical Specifications

Hosting

- Simpleview provides professional website and data hosting at a Tier 1 data facility to support our client, including security measures and traffic analysis by industry leader Google and Omniture when requested.

Application Infrastructure

- Software Architecture
    - Simpleview employs logical tiers for all products to separate presentation layers from business logic and data components.
- Hardware Architecture
    - Simpleview maintains web/application servers and database servers in separate subnets for security.

Accessibility

- Simpleview site designs are always developed to comply with W3C WCAG1, WCAG2 (WAI) and Section 508 accessibility guidelines.

Application Design

- Simpleview has built role-based security into all our technologies. We validate query strings using strong type validation to prevent injection attempts and use IDS devices under firewalls for further protection.

Highlights

- 24 Hour Manned Facility
- Tier I and II Support On-Site
- 5-Tier Security platform
- N+2 for all critical components
- SSAE 16, SAS 70, HIPAA, PCI, FISMA and EU Safe Harbor Compliant Hosting

Application Implementation

Infrastructure Design Requirements

For all our technology implementations, Simpleview uses separate environments for any required development, staging and production. As needed, we can provide network design documents of our production environment/data center.

Web Application Security Within the Software Development Life Cycle

Simpleview offers mature products already in use. Should the need arise, our veteran development environments are protected by thorough security measures.

System and Infrastructure Documentation

Simpleview can provide documentation as required for our existing development and staging environments.

Data Integrity

We place the integrity of client data and our developed data at the highest level of importance in our disaster recovery plan. We established the following efforts to ensure data is always as safe as possible.

Development Environment

In our development environment, we have multiple development servers that store and host our data for testing and development purposes. This data is backed up daily to a local Network Attached Storage (NAS) and replicated to an offsite NAS. In the event of a server failure we are able to recover data from the most recent backup onto another server allowing our Dev teams to continue working on existing projects. The databases are backed up in full weekly with daily incremental backups and transaction log snapshots throughout the day. These database backups are stored on a local NAS and replicated to an offsite NAS.

Production Environment

In our production environment we have multiple web and database servers running and serving our live data. These are either private virtual machines on multiple VMware hosts or physical database servers configured with RAID5 to allow for single drive failure without the loss of data. All private virtual machines are backed up daily using Veeam replication software with periodic daily snapshots. Our databases are backed up in full weekly with daily incremental backups and transaction log snapshots taken throughout the day. This data is stored on an isolated Storage Area Network (SAN) in the data center. All our servers are built into a redundant and fail-over network to ensure maximum up-time, in the event of a primary server failure, the transactions are migrated to a standby server that will continue to manage the site and serve data while the primary is repaired or replaced. This is an automated process, however there is a possibility of momentary service loss resulting from the migration of the services from one server to another resulting in minimal interruption.

Data Center Physical Attributes

Space

- 10,000 square feet total space
- Nine-foot ceiling height clearance
- Raised floors with structural capacity of 1,200 lbs/rack
- Overhead ladder racking
- Zone 1 seismic code construction

Power

- Direct connection to power grid at 13.2 kV
- N+1 electrical design and distribution, including redundant UPS n+1 configuration and battery backup with n+1+1
- Automatic transfer switches ensure smooth transition to backup power
- 72-hour, 750 kW backup generator with 2,300 gallons of fuel onsite, enough capacity to power more than 1,500 homes
- At least 200 watts/sq. ft. density in raised floor area

Environmental Controls

- Manned Facility - Security and Engineers onsite 24/7/365
- Technical support available 24/7,365
- Focused on complex managed hosting environments

Stringent, Multi-layered Security Control Procedure

- 24/7 security monitoring
- Biometric palm scan and photo ID access cards required to enter colocation area. All visitors supervised and escorted.
- 24/7 closed-circuit video monitoring and logging with backup tape storage

Support Connectivity

- Data Center Provides and Maintains All Internet Connectivity for Customers as Part of Service
- 7 diverse fiber paths
- 23 Internet Carriers
- FCP best-path routing

Hardware/Software Based Security

Our network is protected by a four-tier security platform

Tier 1 - Datacenter Border Security

a. Traffic enters and leaves our hosting provider through one of 13 redundant multi-homed Internet carriers and is always routed for best performance.
b. All traffic hits the first line of defense in the 5-Tiered Security, our data center border routers and firewalls. These redundant devices filter known threats, automated attacks, malicious traffic, bogus IPs, bad ports and untrusted networks.

Tier 2 - Intrusion Prevention and Detection

a. If a request makes it through the first tier of security, it enters our hosting providers intrusion prevention and detection systems (IPS/IDS). Here, all requests go through a deep packet inspection and are analyzed for legitimacy.
b. Our hosting providers IPS/IDS systems monitor traffic in real time at gigabit speeds,

and blocks over 2 million attacks per day. Rules are updated routinely and include most zero-day exploits.

Tier 3 - Dedicated High Performance Redundant Firewalls

a. Dedicated high-performance Cisco ASA firewalls are used to achieve complete isolation between environments. Because our security needs are unique, and we are dedicated to the security of our client's data, our staff work directly with the firewall administrators at our data center provider to tune our firewall rules for your data security.
b. Firewalls limit ingress and egress traffic, perform stateful packet inspections and establish VPN connectivity to our offices and for our remote users.

Tier 4 - Enterprise Anti-Virus System

a. The fourth tier works to protect our clients from mistakes and accidents. Our enterprise class anti-virus system uses the latest anti-virus software combined with a host intrusion prevention system to detect and remove viruses and malware from your servers before they can ever execute.

Recovery Plans

a. When possible, the desire is to recover data as rapidly as possible and ensure that the redundancy systems have kicked in and determine the need for intervention. Secondary to that, if there is a system failure, recover data as rapidly as possible to either a standby server or to a server of equal capability to ensure that clients web presence remains online.
b. In the event of catastrophic data center loss, recover the data from the NAS / SAN and begin the process of acquiring and rebuilding servers utilizing disk imaging system to assist with rapid deployment of servers into the domain.

Service Level Agreement (SLA) Structure

1. Server Maintenance
    a. Scheduled Maintenance
        - Simpleview reserves a monthly maintenance window during the third week of the month between the hours of midnight and 3:00 AM Mountain Time for all our North American clients to apply security updates, patches, and other software related updates that require a reboot of a system. Total downtime of a server should not exceed 15 minutes and could occur at any point within this window. For all Clients outside of North America, we will schedule this maintenance as best as we are able in accordance with your work schedules to ensure no disruption of service during your primary business hours. Clients will receive a notification via email at least 24 hours prior to any other scheduled out-of-band maintenance not within this window.

b. Emergency Maintenance
    - If unplanned downtime occurs or is required to restore the availability of any server/services, all efforts will be made to notify clients. Various means of communication will be used, which may include email, forum/blog, tickets, or phone call.

2. Monitoring Service
    - Simpleview employs an enterprise-level monitoring service to alert technicians to any potential issue in availability of any service. Technicians are on-call 24/7 if any alerts are received and issue will be analyzed immediately.
3. Service Level Agreement
    a. Network Uptime
        - Simpleview's data center network has 100% guaranteed uptime in a given month, excluding scheduled maintenance. The data center network Simpleview managed switches, routers, and cabling. It does not include client's local area network or client-provided internet connectivity.

    b. Infrastructure
        - Simpleview's data center HVAC and power has 100% guaranteed uptime in a given month, excluding scheduled maintenance. Power includes UPS's, PDU's, and cabling, but does not include power supplies on your server(s). Infrastructure downtime exists when a particular server is shut down due to power or heat problems.

    c. Hardware
        - Simpleview employs redundant hardware systems where possible to prevent downtime related to hardware failure. If a failure occurs hardware will be replaced at no cost and client will be notified if any downtime results. All hardware has a maximum life of 3 years and is replaced routinely without interruption of service.
4. Response Time
    - Response times indicate when the problem will be addressed, when the client will be contacted, and when resolution will begin. In many cases, the issue will be resolved within the response window. In other cases, it may take more time to troubleshoot and correct an issue, in which case the client will be notified as to the estimated time necessary to complete a request. Response time deadlines will start when the issue is brought to the attention of Simpleview through tickets with an associated response level.
5. Response Levels
    - Critical (Priority 1 – 1 hour)
        - The problem results in extremely serious interruptions to the system. It has affected, or could affect, all users. Tasks that should be executed

immediately cannot be executed because of a complete crash of the system or interruptions in main functions of the system.

- Urgent (Priority 2 – same business day)
  - The problem results in serious interruptions to normal operations. Important tasks cannot be performed, but the error does not impair essential operations; processing can still continue in a restricted manner. The problem hinders productivity by users. The service request requires timely processing, because a long-term malfunction could cause serious interruptions to several users or negatively impact business decisions.

- Important (Priority 3 – next business day)
  - The problem causes interruptions in normal operations. It does not prevent operation of a system, or there could be minor degradation in performance. The error is attributed to malfunctioning or incorrect behavior of the software. The issue will only affect a few users or there is a reasonable way to work around the issue temporarily.

- Minor (Priority 4 – three business days)
  - The problem results in minimal or no interruptions to normal operations (no business impact). The issue consists of "how to" questions, configuration inquiries, enhancement requests, new reports, or documentation questions.

- If Simpleview Technical Support estimates that a reported technical issue or business situation requires additional attention, an internal management escalation procedure will be followed. A management escalation process will be enacted when response-time targets are, or will be, exceeded, when a Work Order is necessary, or when you are dissatisfied with the solution provided.

After Hours and Emergency Contact

Simpleview provides an after-hours line that will alert designated on-call staff members during not business hours based on Arizona/Mountain time. This is to be used to report Critical issues (see definition above) and client will receive a response back within one hour.

In the event of a disaster at ICC, users would be able to access the CRM application from anywhere they have a computer with Internet access.

The Fulcrum Group - Third Party Vendor Support
Disaster Recovery Plan - Availability of Support to ICVB in Disaster

- All of Fulcrum's primary systems have a full disaster recovery plan.

- All critical systems are located at our private data center, ViaWest Data Center, located in Richardson, TX. ViaWest has redundant power, cooling, Internet, and high physical security with multiple disaster recovery plans in offsite locations.

- All Fulcrum employees are setup to work remotely, with full access to all critical systems and data, including telephone system.

Digium Phone System at ICC

This system does not have a backup plan. The best plan for this system is as follows:

- Get a contract/agreement with an answering service.
- Make an agreement in case of a disaster to forward the phones to that service.
- In the event of a disaster, the IT Director or designee would contact Spectrum and have the main phone line forwarded to the answering service and provide the answering service a list of the cell phone numbers of employees.
- Have that service deliver the messages to those employees, until an alternative solution can be reached.

Technical Specifications

- Primary carrier for Irving Convention Center is Time Warner PRI. Backup carrier is Flow route SIP.

Inbound Call Disaster Recovery:

- Inbound calls come in primarily through the Time Warner circuit
- If the Time Warner Circuit is down, ALL calls will failover to the Flow route SIP trunks and will ring into the main desk (ext. 8000 queues).
    - The Flow route number is 972-472-2010. When Primary Circuit is down, Time Warner forwards ALL calls to this number

Outbound Calls Disaster Recovery:

- Outbound calls are sent primarily through the Time Warner circuit.
- If the Time Warner Circuit is down, the outbound calls are sent out via the Flow route SIP trunk.

The above failover routes should be unnoticeable by the users except that during failover, the inbound calls ALL ring to the main number.