Call Center Site Certification Criteria

Developed by SNUG for Startel Soft Switch Sites

General Business Practices

Licenses & Memberships

1. The site is required to be a SNUG member in good standing. SNUG membership dues must be fully paid up to and including the year of the certification.
2. A valid business license, if required by state or local government.
3. Proof of business and workmen's compensation insurance.
4. Proof of errors and omissions insurance.

Safety

1. The site is required to comply with local building codes. No obvious violations such as narrow doorways, low ceilings, unmarked stairways or exits, etc.
2. The site must have fire extinguishers located within sight distance of every fire exit, not to exceed requirements of any local authority having jurisdiction.
3. Low voltage backup lights/exit signs must clearly illuminate emergency routes and all fire exits.
4. An evacuation plan and diagram must be posted including the location of fire extinguishers, pull stations and exit route arrows.
5. The site must have smoke detection (photo electric type suggested or be part of a certificated alarm) along paths of egress that can be heard in the operations room(s) or anywhere an agent is likely to be.
6. Carbon monoxide detectors must be present in the operations room(s) or anywhere an agent is likely to be.

Personnel

1. Written employee manual covering all employment related issues that has been revised within the last 12 months.
2. Written hiring procedures revised within the last 12 months. These procedures are not set by SNUG, but should comply with all local, state, and federal laws.
    a. Include items like: Standard application, interview questions, test scoring levels, etc.
    b. SNUG recommends that these guidelines be developed with appropriate legal counsel.
3. Written procedures for terminating employment of individuals (full-time, part-time, temporary, contractors, etc.) including:
    a. Disabling of any PHI user accounts such as Agent Interface, Admin Controls, Intellisite, etc.
    b. Disabling of Windows accounts to workstations and/or servers
    c. Termination of any other system access
    d. Conduct exit interviews
    e. Retrieval of all organizational property
        i. Returning old and issuing new keys, identification cards, and building passes, hard drives, laptops, desktops, USB drives, etc.
    f. Provide appropriate personnel with access to official records created by the terminated employee that are stored on the information system (i.e. computer, server, etc.)

HIPAA

1. Incorporate the use of nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of interest agreements.
2. Write policies and procedures that specify how and when access is granted to PHI systems, such as Agent Interface and Admin Controls so that PHI is transmitted in secure & encrypted format.

3. Security awareness training to all users before authorizing access to the system, i.e. during new employee orientation.
    a. Examples of providing information security reminders include:
        i. Face-to-face meetings
        ii. Email updates
        iii. Newsletters
        iv. Postings in public areas, i.e. hallways, kitchen
        v. Company Intranet
        vi. Security awareness training should be conducted at an on-going basis
4. Reporting of incidents to the appropriate personnel, i.e. designated Privacy Officer or Information Security Officer.

Training & Education

1. Attend at least one SNUG conference every two years.
    a. At least one employee of the site must attend a full SNUG conference.
        i. A partial training day at the conference shall not be satisfactory of this requirement.
2. Incorporate a custom supervisor training program or participate in the TEAM SNUG 24/7 Certified Supervisor program.
3. At least one current employee of the site must have completed the following training classes:
    a. CMC Admin Training
    b. Soft Switch Technical Training
        i. A written test may be taken as an equivalent for either test if available from Startel.
4. Demonstrate one of the follow options for the site’s agent training program:
    a. Participate in the ATSI Agent & Advanced Agent Certification program.
        i. Verify that 75% of the eligible agents have successfully completed the program.
    b. Demonstrate the site’s agent training program, process & materials such as:
        i. Training Manual
        ii. WBIT
        iii. DVDs / Videos
        iv. Online resources
    c. OR, as a replacement have detailed internal documentation for Agent & Supervisor training procedure.
5. Recommended participation in the ATSI and / or CAM-X Award of Excellence

Evaluations

1. Specify written criteria for the following evaluations:
    a. Who is to be evaluated?
    b. What is to be evaluated?
    c. How frequently are evaluations to be completed?

Operations

Equipment

1. Site must be running on a currently supported version and platform of Startel software.
2. Configure the site to have CMC A & B servers and SS A & B servers. The A and B servers are designed to create a primary and a backup server scenario capable of running the site’s day to

day operations. Automatic failover is not required, but the ability to utilize either A or B servers as the primary servers shall exist.

If B servers are not available, an alternate Business Continuity plan should detail how to continue operations in the event of a failure of the single CMC or SS, and the provisions for this plan should be available. For example, sites that utilize Startel Disaster Recovery service must verify the DR system is up to date and connectivity is successful.

3. The site's Startel version number must be within one version number from the current Startel version, i.e. if Startel's current version is 12, the site must be running Startel version 11 or greater. If the site is beyond one version number, the site must upgrade.
4. All PC and servers must be within a supported OS manufacturer life cycle. PC and servers running an OS outside of a supported manufacturer life cycle must be upgraded.
5. Spare parts available. To include at a minimum of:
    a. USB keyboard with Startel keys identifiable. Keyboard sticker labels will be adequate.
    b. Polycom phone, equivalent IP phone or Startel soft phone installation files
    c. Startel Agent Interface, Admin Controls, & STL Common files with the current build
    d. Agent Headset
6. Voice logger capable of recording all inbound and outbound calls.
7. A tool kit to include at a minimum:
    a. Philips head screwdriver
    b. Flat head screwdriver
    c. Wrench or nut drivers (small & medium size)
    d. Flashlight.
8. Have on-site generator or access to a generator capable of being on-line within half the run time period of the UPS.
    a. The name and telephone number of a vendor who can supply the site with a standby generator should be located in the operations room(s) and server room(s) in the event the site does not own an on-site back-up generator.
    b. If transfer to generator is not automatic, site should have posted procedures to include:
        i. The location of proper extension cords to power UPS, if required.
        ii. Work light available in equipment area.
    c. If the Business Continuity plan calls for a geographically diverse system to come online and allows for the abandonment of the primary office, then that switchover must be achievable within half the run time period of the UPS.
9. The site must have at least two workstations and the primary operation servers connected to UPS with the capacity to run for a minimum amount of time required to start the back-up generator.
    a. A standby electric generator with transfer switch is an acceptable substitute for runtime requirement as long as there is no interruption of power.
    b. An acceptable option would be to provide a solution for remote agent access so that agents may continue to operate while the site's power is down. This should be documented in the Business Continuity plan. For example, a geographically diverse office or individuals.
10. Maintain an air conditioned server room.
    a. Implement a temperature alarm monitor to audit the server room temperature.

        i. Products like a wireless temperature sensor provide the ability to log room temperature and humidity levels. These sensors can send notifications to email addresses or text messages when certain thresholds are reached.
            1. www.lacrossetechnology.com/sensors.php

11. Software capable of the destruction of hard drives, removable media, etc., including:
    a. Physical destruction.
        i. Companies like Retire-IT that offer these services and also come onsite to destroy media.
    b. DoD wiping of media before reuse. DoD wiping should also be performed even before destroying media. DoD wiping involves writing over the hard drive with random data 7 times before it's considered unrecoverable. http://en.wikipedia.org/wiki/Data_erasure
        i. Programs like Darik's Boot & Nuke or Blancco provide adequate solutions for data erasure.
12. Implement an A/B toggle switch for any PRI's connected to SS A & B. Utilizing the toggle A/B switch makes failing over from A to B easier without having to physically move cables from one server to another.
    a. 2 Ports/2 Way 8P8C RJ45 Network/Ethernet Manual AB Share Sharing Switch Box
    b. A switchover procedure that clearly describes and indicates how to switch PRIs from one server to another is acceptable. In most cases, pictures of the cabling is helpful.

Network Security and Remote Access

1. The site shall have at least two sources of high speed Internet via DSL, cable modem, T-1, or fiber with at least one static IP address.
    a. Maintain a backup high speed Internet source of equal quality and at least one static IP address.
        i. The Site shall employ the use of a firewall appliance such as Cisco, WatchGuard, Sonic WALL or Symantec capable of managing two high speed Internet wide area network (WAN) Connections and one internal LAN. The firewall appliance shall scan all inbound and outbound connections at the Internet gateway for viruses and shall employ intrusion detection technology.
        ii. Because of the wide range of products and services offered, the examiner shall have latitude in determining compliance. The intent of this section is to demonstrate Internet redundancy (automatic failover), and intelligent firewall protection for both Internet gateways.
2. The site shall have a suitable router or firewall appliance capable of performing network address translation from public IP addresses to private local area network (LAN) addresses. All PC and servers on the LAN shall have static 192.168.xxx.xxx or 10.xxx.xxx.xxx IP addresses assigned and not use DHCP. Such addresses shall be listed or otherwise diagramed to easily locate PCs and servers by location.
3. Access to an office server or workstation with a encrypted and secure connection   Example: your firewall should not have TCP port 3389 (or similar) opened (forwarded) to any server or workstation in the site or call center.
4. Use of SSL/TLS for web-based access to PHI software.
    a. Intellisite must have SSL certificate.
    b. This includes web based remote connections, as well as to web access given to clients, partners, or vendors to any website available on the public Internet such as Appointment Scheduling software and Secure Messaging Plus.

5. All PC and servers within the LAN or used for remote access shall have a current subscription based licensed version of antivirus software and anti-malware installed. All PC and servers must have up-to-date virus definition files.
    a. Endpoint security solutions (i.e. McAfee Enterprise, Cisco CSA, Symantec Endpoint, etc.) have the ability to prevent unauthorized modification to software running on the computer or server.
6. Report of incidents of security or network breaches to the appropriate personnel, i.e. designated Privacy Officer or Information Security Officer.
    a. Review the activities of users by utilizing auditing functions, Windows Event Logs, and networking logs from routers, switches, and firewalls.
    b. Use of central syslog server for monitoring and alerting of audit logs and abnormalities on the network, including items such as:
        i. Account locked due to failed attempts
        ii. Failed attempts by unauthorized users
        iii. Escalation of rights
        iv. Installation of new services
        v. Event log stopped
        vi. Virus activity
        vii. Account creation
        viii. Account modification
        ix. Account disabled
        x. Account escalation
        xi. Server health
        xii. Network health
        xiii. Access allowed
        xiv. Access denied
        xv. Service installation
        xvi. Service deletion
        xvii. Configuration changes
7. Create a policy and process for disabling and removing accounts for voluntary and involuntary terminations.
8. Passwords include tokens, biometrics, and certificates in addition to standard passwords. Standard passwords should meet the following criteria:
    a. Enforced in the PHI systems (Agent Interface & Admin Controls), Active Directory, or at least on the local workstation or server level.
        i. Enforce password history. Recommended: Previous 3 passwords cannot be used.
        ii.
    b. Minimum password length. Recommended: 8 or more characters long
    c. Password complexity. Recommended: Passwords should contain 3 of the following criteria
        i. Uppercase characters (A-Z)
        ii. Lowercase characters (a-z)
        iii. Numbers (0-9)
        iv. Special characters (i.e. !, #, &, *)
    d. Account lockout. Recommended: Accounts lock after 3 unsuccessful password attempts

9. Passwords include Microsoft logins (Active Directory Domain Controller or just locally logging into a computer) for each individual user. Unique username and password for PHI systems. The use of passwords and/or tokens for remote access through a Virtual Private Network (VPN) is required for remote access.
10. There should be no shared access for any resource or system (i.e. computer or PHI system).

Support & Troubleshooting

1. Proof of current Startel support contract.
2. Hardware support for the primary Startel servers. (Provided by Startel and/or server manufacturer and/or equivalent.)
3. Startel Technical Support telephone number and email address along with the site’s 6 digit Startel account number displayed in the operations room(s) and server room(s).
4. A direct telephone line or cellphone to reach the operations room(s) or server room(s) that is not routed through the Startel switch with the number prominently displayed.
5. Maintain a backup digital or hard copy of current instructional system manuals.
    a. Startel Admin Controls & Agent Interface
    b. Server maintenance
6. Remote access program Bomgar must be available to Startel Technical Support to access the primary Startel related servers.
    a. CMC A & B
    b. SS A & B
    c. Web Server hosting Intellisite (if applicable)
7. Written policy for the site’s maintenance schedule:
    a. Maintenance duties clearly assigned and a place to sign off as they are completed.
    b. CMC A & B
        i. Windows Updates
            1. Frequency
            2. By who
    c. SS A & B
            1. Linux Updates
            2. Frequency
            3. By who
    d. Startel system content (Messages, Locates, Ifs, IntelliForms, etc) must be routinely archived.
        i. These categories can be archived via Admin Controls > System Settings > Auto Maint. Settings.
        ii. Verify that auto archiving policies are running. If a manual process is in place, review the logs of dates and what was archived.

Backup & Restoration

1. The accepted rule for backup best practices is the 3-2-1 rule. It can be summarized as: if you’re backing something up, you should have:
    a. At least three copies:
        i. Three different copies means three different copies in different places. (Different folders on the same hard drive or flash disk does not count.) Why three? In the digital era, it is very easy to make digital copies, and it’s better to

have more copies than too few. By keeping them on different places, it reduces the risk of a single event destroying multiple copies.

- b. In two different formats,
    - i. Now, why two different formats? What this means is that you must use at least two different methods to store your data. For example, burning your photos to a DVD from your PC's hard drive counts (hard disk and DVD). However, copying them to an external disk does not (as they're both hard disks.) If you do both, then you satisfy this rule (and the first one as well). Again, using different formats reduce the risks that all your backups will be damaged, as different formats have different strengths and weaknesses when it comes to redundancy.
- c. Off-site or cloud-based copies of back-ups
    - i. Keeping one copy off-site ensures that even if something happens to where your data is – like a fire, or a break-in – at least one copy is safe somewhere else. If something does go wrong where you are, at least your data will be safe.
- d. Perform nightly backups of vital data which are taken offsite (cloud backup) daily, at a minimum weekly.

2. Implement a bare metal backup and restoration process for the operating systems of the primary Startel servers.
    - a. Programs like Acronis create a full image of the OS for your server and workstations
    - b. Bare-metal recovery ensures that you are back up and running in minutes, not hours
    - c. Create a bootable DVD/USB with an ISO (or equivalent) with the current OS and drivers.
3. Maintain current backups (Backups shall be completed under the 3-2-1 rule) for some of the following data:
    - a. Soft Switch configuration files
        - i. Asterisk
        - ii. Dahdi
        - iii. Polycom
        - iv. Repos
        - v. Startel
        - vi. Vmail.sql
    - b. SQL databases
        - i. STLNTDB
        - ii. System databases (master, model, msdb, and tempdb)
    - c. Account & system voice greetings
    - d. Call recordings
    - e. Startel system data (Mastercards, Messages, Locates, Ifs, Intelliforms, Client contact names and transports)
    - f. DID number to client assignments
    - g. Routing table assignments
    - h. Scenario assignments
4. Confirm that Soft Switch data is syncing between the primary and backup soft switches (RSYNC)
    - a. These syncing jobs shall be scheduled daily/nightly.
    - b. These jobs can be found on the primary Soft Switch server in the "crontab" folder.
        - i. #cd crontab –e
    - c. Jobs shall include but not limited to:
        - i. Move yesterday's API logs to old and compress them

        ii. Compress logger clips
        iii. Backup switch data to CMC
        iv. Rsync to backup SS, if applicable.
        v. Remove old APIserver logs
        vi. Remove old voicemail messages
        vii. Logger daily backups and purges

5. Implement a high availability mode in MS SQL between CMC A & B server. Utilize database mirroring or Always-On High Availability.
6. Backups are only as good as your recovery process. Implement procedures for periodic testing and revision of contingency plans.
    a. The training of personnel in their contingency roles and responsibilities.
    b. Training should occur at least annually.
    c. Testing of the contingency plan at least annually, i.e. a table top test to determine the incident response effectiveness and document the results.
        i. Download cloud based backups or return off site backups to the site location
        ii. Restore a copy of the STLNTDB database (this shall be to a separate test database and not the live STLNTDB)
        iii. Load a bootable DVD (or other media) to launch an OS of primary Startel servers
            1. Programs like Acronis can create bootable media.
    d. Document and review the contingency plan at least annually and revise the plan as necessary (i.e. based on system/organizational changes or problems encountered during plan implementation, execution, or testing.
7. Maintain a backup / alternate source (SMTP account) from a separate provider for sending email.
    a. Companies such as www.sendgrid.com or www.smtp2go.com provide a subscription-based SMTP service.

Emergency Procedures

1. Written procedure in case of a power down of the system/switch would be necessary to run directly from a back-up generator. Include directions describing how to connect system equipment to generator.
2. Document a paper call taking system in case of an event of an extended loss to the data servers.
    a. How will the site process messages?
    b. How will the site dispatch messages?
3. Emergency procedure manual shall be clearly marked and located in site's equipment/server room. This manual is to contain:
    a. Contact names and numbers of site technical and key management personnel.
    b. Contact names and numbers for Startel, Telco, & other vendors, including relevant account numbers.
    c. Current software and firmware levels, including dates of previous upgrades.
    d. History of system maintenance on primary servers, and major upgrades.
    e. Include Startel service history to include previous system troubles, the cause and what fixed the problem. Startel Tech Support should be able to provide a list of opened tickets for the site within the previous year.
        i. Startel Beta sites do not need to include Beta issues reported to Startel Tech Support.

f. List the location of system spares parts. See the spare parts section listed under equipment.
    i. System spares shall be clearly labeled and stored appropriately.

g. List the locations of the 3-2-1 backups. See the list of items to be backed up in the Backup & Restoration section.
    i. Include the physical or cloud location.
    ii. Include the necessary contact information.
    iii. Include the necessary credentials to access the information.

h. List the location of all system manuals.

Supplemental Information

1. Any requirement not allowed by local or state ordinance shall be waived.
2. Use of a service agreement with terms and conditions including Limitation of Liability in initial contract and periodically included with invoices.
3. Attend the SNUG Conference each year for Gold Certification.