NAI Global's Colocation Strategy:

NAI Global utilizes a 3rd party colocation provider to host its primary data and application servers. Our colocation provider is an ISO: 9001:2000-certified provider employing over 300 proprietary ISO-compliant processes for network management, monitoring and disaster recovery. The primary NAI Global servers are monitored by the collocation provider on a 24x7, 365 days a year basis. The NAI Global servers are monitored for network / internet connectivity issues, security threats, and application faults.

In addition to the primary servers being hosted at our colocation site, NAI Global maintains mirror servers at its corporate locations and has redundant internet connections in this location. These mirror servers contain copies of all systems and application software, and the database components are continuously synchronized through the database management system. Document attachments are synchronized 1 – 2 times daily.

This remainder of this document describes in greater detail NAI Global's backup / restore methodology and provides response instructions for various events that may occur. NAI Global's disaster recover plan covers issues from simple programming bugs to catastrophic building failures at our colocation provider. The policies outlined are designed to provide maximum protection to all data hosted by NAI Global and to minimize server downtime in the event of critical errors and catastrophes.

System Files / Application Data Backup Strategy:

NAI Global employs a multi-tiered backup strategy that is made up of the following components:

- **Application-based logging** –all changes posted to the database are logged to a separate transaction log maintained by the application. This log is primarily used to security and auditing purposes and can also be used to reconstruct the database if needed.

- **SQL Server-based transaction logs** – all changes made to the database are also kept in a SQL Server-based transaction log. This log is used to restore data up to the point of failure, if possible.

- **Nightly tape backups** – all system and data files are backed up to tape on a nightly basis. In the event a restore from tape operation is required, the tape backups are used to restore data files, system configurations, etc. and the SQL Server transaction logs are then applied to restore the database to its condition at the time of failure.

- **Server-based disk backups** – all NAI Global servers are configured with hot-swappable backplanes and RAID disk controllers. In the event of a hard disk failure, disks can be swapped in / out as needed and the RAID system handles the recovery / reconstruction of each disk's contents

- **In-house Server-to-Server backups** – each primary server (i.e., SQL server machine, Web server machine, communications server machine) in the NAI Global network has a secondary sever which is kept in sync with the primary. In the event one of the primary servers goes offline, the secondary server can be brought online immediately.

- **Remote Server-to-Server backups** – a copy of all systems and server software, as well as the database maintained on a separate, remote server. Database contents are automatically synchronized. Document attachments are synchronized 1 – 2 times a day.

NAI Global maintains specific recovery plans for specific types of catastrophic events. The remainder of this document provides detailed implementation plans for each type of catastrophic event.

Tape Backup Operational Notes:

Full system and data backups to tape are performed on a nightly basis for all primary and secondary server systems in the NAI Global data center at our colocation facility. NAI Global also performs full system and data backups of our backup servers located in NAI Global's corporate headquarters.

Current backup tapes are kept in a secured, offsite location.

Historical backup tapes are kept on location in a fireproof safe.

Nightly backups include all databases, servers, and system files. All backup tape contents are virus checked by virus checkers on both the source server, as well as the backup tape software itself.

All backup tapes are encrypted and password protected.

Backup tapes are retained according to the following schedule:

Daily:	2 weeks
Weekly:	1 year
Monthly:	2 years
Quarterly:	5 years
Annual:	10 years

System Recovery Procedures:

NAI Global's recovery procedures are in effect for various events and are designed to cover system failures that range from a simple programming bug to a catastrophic building failure. The primary objective of the NAI Global Backup and Recovery Procedures is to prevent data loss and keep server downtime to an absolute minimum.

The following sections describe each event and the appropriate recovery plan.

Event Type: Application Program Fault

Event Severity: Minimum to Severe / Non-catastrophic

(Severity level depends upon root cause and potential recovery steps required to resolve.)

All applications software is vigorously tested prior to being released to a production server. Application program faults themselves are rare, application program faults that affect the entire network are extremely rare.

Estimated Time Of Recovery: Immediate to 4 – 6 hours.

(Recovery time depends upon root cause and recovery steps required.)

Recovery Plan: The following steps are to be taken:

1. Evaluate problem and take servers offline, if required, until root cause is determined.
2. Contact systems administrator and inform of situation.
3. Determine root cause of problem (i.e., programming bug, data corruption, other).
4. Resolve issue – fix programming, recover any lost data from backup tape and restore SQL server transaction logs created since last backup set was created.
5. Test any fixes to ensure problem has been resolved.
6. Bring servers back online.
7. Complete a Systems Event Report.

Event Type: Server Hard Drive Failure

Event Severity: Minimum / Non-catastrophic

All server hard drives are configured with hot-swappable backplanes, and RAID 1 – 5 controllers. All system and data drives are mirrored within a single system.

Estimated Time Of Recovery: Immediate.

Recovery Plan: The following steps are to be taken:

1. Remove appropriate hard drive from affected server.
2. Contact hardware manufacturer to have replacement drive shipped overnight.
3. Verify all other primary and secondary servers are functioning.
4. Replace bad hard drive with new drive, once it arrives.
5. Complete a Systems Event Report.

Event Type: Server Failure

Event Severity: Severe / Non-catastrophic

Each NAI Global server has primary and secondary server hardware. The primary and secondary servers have identical configurations, which allows for swapping parts and hard drives between them.

In the event of a server failure, the secondary servers will be immediately brought online.

Estimated Time Of Recovery: Immediate to 4 – 6 hours.

(Recovery time depends upon root cause and recovery steps required.)

Recovery Plan: The following steps are to be taken:

1. Evaluate problem.
2. If server cannot be immediately recovered, bring secondary servers online and update appropriate DNS entries to reroute traffic to secondary server.
3. Verify secondary systems are online and accessible to both internal and external users.
4. Contact Systems Administrator.
5. Evaluate transaction logs (if possible) to verify data and protect against data loss between the primary and secondary servers.
6. If needed, recover any data from tape backup systems.
7. In the event of data loss that cannot be recovered (i.e., transactions being processed at time of failure), notify appropriate users of event and steps they need to take to reenter any information.
8. Contact hardware manufacturer for service dispatch.
9. Contact hardware manufacturer to have replacement drive shipped overnight.
10. Work with hardware manufacturer to isolate problem and acquire replacement parts, as needed.
11. Complete a Systems Event Report.

Event Type: Primary Internet Connectivity Loss To Main Data Center

Event Severity: Severe / Non-catastrophic

The primary NAI Global servers are hosted at an offsite location which maintains several connections to the internet. Each of these connections is connected to both the primary and secondary server systems and each server is monitored 24x7, 365 days a year by NAI Global's colocation provider.

This section describes the loss of internet connectivity to our colocation provider.

An event resulting in long-term (more than 1.5 days) connectivity loss to our primary servers hosted offsite would be considered a **Catastrophic Building Event**,

Estimated Time Of Recovery: Immediate.

Recovery Plan: The following steps are to be taken:

- Work with colocation providers to diagnose and fix problems.

If problem is NAI Global owned equipment:

1. If the problem is related to NAI Global owned equipment, use secondary routing equipment, if available, and contact hardware manufacturer for immediate replacement of affected equipment.
2. Work with hardware manufacturer to get replacement parts delivered and installed.
3. If needed, update appropriate DNS entries / routers to reroute traffic
4. Send broadcast message to NAI Global users informing them of connectivity problems and to use the secondary server address names (i.e., www2.naiglobal.com, members2.naiglobal.com) until primary ISP reroutes traffic to secondary connection.
5. Complete Systems Event Report.

If problem is related to colocation provider:

1. Contact colocation provider to determine root cause and estimated time of repair.
2. If needed, have primary ISP reconfigure routing to reroute traffic to secondary ISP connection.
3. Send broadcast message to NAI Global users informing them of connectivity problems and to use the secondary server address names (i.e., www2.naiglobal.com, members2.naiglobal.com)
4. Complete a Systems Event Report.

Event Type: Catastrophic Building Failure

Event Severity: Disastrous / Catastrophic

In the event of a disastrous event occurring to the NAI Global data center site (i.e., fire, earthquake, etc.) that results in a significant loss of internet connectivity (1.5+ days), NAI Global maintains a mirror copy of all applications software and server software (database server, tape backup server software, web server and applications software, and messaging server and software) as well as database items at it's corporate office location.

In the event of a Catastrophic Building Failure NAI Global the backup servers located at NAI Global's Corporate Headquarters can be brought online.

In the event that catastrophic failure is part of a broader regional catastrophe, NAI Global's colocation provider has world-class data centers in 13 major markets across the US. If conditions warrant, new sites can be placed in one of these other locations by shipping servers to one of these locations.

Estimated Time Of Recovery: Currently 2 – 6 hours.

Recovery Plan: The following steps are to be taken:

1. Work with colocation provider to update DNS entries to route traffic to backup sites located at corporate headquarters.
2. Verify backup sites are accessible to external users.
3. Send broadcast message to NAI Global users informing of situation and status and how to reach the backup servers.
4. Depending upon situation, prepare new data center site and obtain / configure replacement servers as soon as possible.
5. Work with hosting provider Test new primary data center site as soon as possible and take steps to bring primary servers back online.

Email Services

NAI Capital email services are housed by a 3rd party colocation provider. Our provider is ISO/IEC 27002 and ISO/IEC 27001 certified, their U.S., U.K and Hong Kong data centers have passed SSAE16 Type II SOC1, SOC2 (Security and Availability only) and SOC3 audits.

System Files / Application Data Backup Strategy

NAI Capital employs multi-tier backup strategy based upon the type of system and data that requires retention or needed for business continuity.

- Backup Locations and Media Types
  - On-Site Backup: two separate discreet systems, a primary and backup (from the prior business day) to enterprise level hard drive RAID 5 network-attached storage devices.
  - Off-Site Backup: Off-site backups are synchronized on a daily basis with our 3rd party colocation provider who is ISO 27001 certified and has passed SOC1 audits. Data is kept for a minimum of 90 days

- Critical Accounting Systems:
  - Accounting systems are backed up on an hourly basis with full backups on a weekly basis.

- Project File Systems

We have the flexibility to backup as needed for project file systems used locally in-house. We can customize a backup & recovery solution to meet the needs of each client.

  - Project File Systems are stored on two discreet systems; a primary and backup (from the prior business day). All files are backed up to enterprise level hard drive RAID 6 network-attached storage devices.
  - Project File Systems are synchronized daily with our 3rd party co-location provider who is ISO 27001 certified and has passed SOC1 audits.
  - For NAI Capital to provide Backup and Recovery all data must be stored on our network-attached storage and not on individual desktop or laptop computers.
  - For shared systems with external users we use NAI Global provided REALTrac. Please consult the NAI Global Backup & Disaster Recovery Plan for more information about REALTrac.

- Network Security
  - NAI Capital is open to discussing network security after all parties sign a Non-Disclosure application. Please contact your broker for more information.