Remote
Disaster Recovery
Services Suite *(nVision Edition)*

- Services Suite includes Remote Backup Service
- Comprehensive suite of services designed to get you back up and running quickly and successfully
- Supplies a temporary nVision environment in the event of a disaster
- Offers off-site restore capabilities for your nVision data
- Protects your nVision data with best-practice business continuity methods
- Provides the ability to perform test restores for remote data verification

Remote Disaster Recovery Services Suite (nVision Edition)

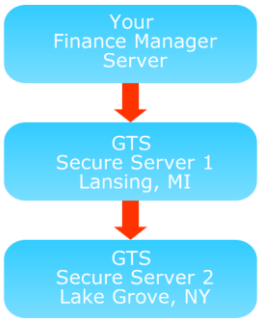
Overview

Our solution is a comprehensive suite of services designed to get you back up and running quickly and successfully. This services suite includes our Remote Backup Service. We also provide a temporary off-site nVision environment in the event of a disaster. The services suite also protects your nVision data with best-practice business continuity methods.

Features

- ### Remote Backup Service

  Your nVision data is securely backed up to our primary server on a nightly basis. The service also provides restore and remote data verification capabilities to test your backups. Periodic random restores are also performed by Granite Tech Solutions.



- Scheduled, secure, logged transfer of your encrypted nVision data to our secure remote server in Michigan, more than 300 miles from your district or municipality
- Our secure primary backup server is housed in an industry-leading and SSAE-16 (formerly SAS70) audit compliant data center facility in Lansing, MI
- Backups are synched to our secure server in Lake Grove, NY for redundancy

- Servers are configured with RAID redundancy (this provides fault tolerance which helps protect your data if a hard drive fails)
- Backups occur in the evening during off-peak traffic times, 7 days a week
- Nightly backups are stored for 14 days
- Minimal configuration is required
- Technical support is available by phone M-F from 9am-5pm EST

NOTE: This information is subject to change as we continue to make changes and improvements to our service.

P: 631.739.6272 · F:631.615.0028 · SALES@GRANITETECHSOLUTIONS.COM · GRANITETECHSOLUTIONS.COM

Remote Disaster Recovery Services Suite (nVision Edition)

- **Remote Backup Service (continued)**

- For Data Verification Restore requests, we provide remote access to an nVision environment; All activities are logged.
- We will randomly test your backups to ensure they are valid and usable data archives; All activities are logged.
- Daily automated monitoring of your backup job and auto-notification upon backup failure
- Contract includes GTS Backup Agent - nVision Edition software

- **Mobile Workstation**

In the event of a reported disaster, **we will send you a laptop pre-configured with nVision and your most recent data, a LaserJet printer with standard toner and CD-Rs and/or DVD-Rs for data backup.** You will also receive MICR toner and blank check stock for printing upon request.





- Use of requested **Mobile Workstation** for up to 30 calendar days from shipping date*

Other Features

- We have implemented data security and handling policies specific to nVision data
- Our solution exceeds the New York State Comptroller's recommendations for disaster recovery of your nVision software

* Some restrictions/limitations apply. Please contact our sales department for details.

Remote Disaster Recovery Services Suite (nVision Edition)

System Requirements:

- A Windows server the current version of nVision Software.
- 7Zip (this is a free open-source archiving program)
- WinSCP (this is a free open-source FTP program)
- Access to an account on that server with Administrator rights/access. This is required to install and run our backup agent.
- Network access to configure/enable connections to a remote FTP server

Why choose Granite Tech Solutions?

- We offer a tested disaster recovery solution, not just remote backup for your nVision data.
- We have consulted with Finance Manager, independent auditors, and other industry experts to assemble the most comprehensive solution for your nVision data.
- We have consulted with private auditors, school business officials, superintendents, and industry experts to determine the needs, requirements, and best practices for successful disaster recovery.
- Our staff has over 20 years combined experience in data backup, project management, web hosting, networking, and software development. Our staff also has networking experience within schools in New York State.
- We are family owned and operated and offer a personalized level of service that only a local solutions provider can deliver and that you can trust.
- We will get you up and running quickly and successfully.

We encourage you to ask the following of <u>any</u> disaster recovery service provider for nVision:

- ❑ Do they own a valid nVision Software license for in-house use?
- ❑ Have they tested and confirmed that their solution works?
- ❑ How do they keep up-to-date with the latest code and software updates for nVision?
- ❑ Do they provide your district with the ability to perform periodic restores of your nVision data to a non-production nVision environment for data validation?
- ❑ If yes, do they allow you to do so remotely?
- ❑ In the event of a disaster, will they provide you with access to a workstation pre-configured with your latest restored nVision data and a printer?
- ❑ If yes, will they send this environment to you?
- ❑ Have they worked with Finance Manager and to develop their solution? (Granite Tech Solutions has worked extensively with Finance Manager to develop our solution)
- ❑ Does their solution address the Division of Local Government and School Accountability's recommendations for having a remote backup **AND** remote disaster recovery solution for their financial data?
- ❑ Are their current clients satisfied with their services? Can they provide references?

With Granite Tech Solutions, the answer is "YES" to all of the above.

General FAQ's

Q: ***What are we talking about when we say "disaster?"***
A: A disaster is any event (whether due to natural or man-made causes) that interrupts operations that are critical to conducting business for 24 hours or longer. The range of disaster impact can vary greatly, depending on the type of event. We consider them in three categories:

- **Limited:** hardware, software and equipment (theft, accidental damages, failures, viruses, malicious access)
- **Localized:** effects only buildings in your district or municipality (networks, fires, floods, lightning strikes, local power outages)
- **Regional:** effects all districts and municipalities in the area (hurricanes, blackouts, major floods, snow events, tornadoes)

Q: ***What is disaster recovery?***
A: An integral part of business continuity, it's the processes, policies and procedures of restoring operations which are critical to resuming business.
It encompasses the following:

- **Regaining access to critical data** (records, hardware, software, networks, etc.)
- **Restoring communications** (incoming/outgoing, phone, fax, internet, etc.)
- **Restoring work spaces and other business operations** (financial and administrative software systems)

Q: ***What is a disaster recovery plan and why do I need one?***
A: A Disaster Recovery Plan is designed to avert or minimize the damage that disasters would cause to your operations. It involves more than just preparing for a move off-site after a disaster. These plans address the cost and time loss associated with recovery and Recovery Time Objectives (RTO). The plan is designed to address how to keep critical functions operating in the event of disruptions, both large and small. It also consists of precautions taken so that the effects of a disaster will be minimized, and reduce the risk of potentially losing important financial and administrative data.

The New York State Comptroller's Office Division of Local Government and School Accountability recommends the following:

- Districts/municipalities have a Disaster Recovery Plan consisting of advance decisions on what, how, when, and who are needed to provide a solution that will sustain critical business functions. The plan should include precautions to be taken to minimize the effects of a disaster so that the organization will be able to either maintain or quickly resume mission-critical functions. Such planning involves more than preparing for a move offsite after a disaster.
- Districts/municipalities develop and adopt a Comprehensive IT Policy relating to Data Backup and Disaster Recovery that addresses the range of threats to your IT system, including specific details or critical components such as an alternate processing site and the security of backups
- Districts/municipalities have a Remote Disaster Recovery Plan [included in a business continuity plan] in place for *Financial Data and Software Systems* and *Administrative Data and Software Systems* that describes specific guidelines for the protection of essential data against damage, loss, or destruction
- Verify that backup data is periodically tested and restored to ensure that it is complete, accurate, and usable

Q: *What is the GTS Remote Disaster Recovery Services Suite, in general terms?*
A: It is a comprehensive suite of services designed to help protect your Finance Manager data and get you back up and running quickly. This is facilitated by providing a complete temporary working nVision environment in the event of a disaster. It is comprised of two services: Remote Backup Service and a Mobile Workstation.

Q: *How does Granite Tech's solution for nVision address my need for disaster recovery?*
A: We backup your data in multiple, geographically dispersed locations and verify that your backups are usable by performing periodic restores. In the event of a disaster, we provide you with hardware and software access to get you up and running quickly by sending you a "mobile workstation." We also provide you with formalized checklists to follow in the event of a disaster in any of the aforementioned categories. We have consulted with private auditors, school business officials, superintendents, and industry experts to determine the needs, requirements, and best practices for successful disaster recovery. On a regular basis we review: the audits by the Division of Local Government and School Accountability, our company policies, and our solution procedures to provide our clients with the best solution available. We have also consulted extensively and worked with Finance Manager to develop our solution.

Q: *What does my service contract include?*
A: Your Service contract includes the following:

- Our services are available after only 24 hours of inability to access your nVision environment
- Nightly redundant backups stored for 14 days
- Redundant backup at industry-leading facility (Lansing, MI datacenter)
- For non-disaster-related restore requests, we provide remote access to a nVision environment
- Performing of random periodic restores and testing of files for formatting validity
- Use of requested mobile workstations for up to 30 calendar days from shipping date
- Contract includes GTS Backup Agent- FM Edition
- Installation support, implementation support, and technical support

Q: *How long does it take to set up this service from Granite Tech Solutions?*
A: Typical implementations are completed within 30 business days of the effective date of your signed service agreement.

Q: *What if I need technical support?*
A: Call us during normal business hours.

Q: *How do I print checks in the event of a disaster? How does that work?*
A: That process has been formalized and we provide our clients with step-by-step worksheets. (See FAQ's-Technical)

Q: *How do I know that the backup is working and usable?*
A: We perform our own random restores on a periodic basis and recommend our clients do too. We also closely monitor daily backup files. (See FAQ's-Technical)

Q: *If I have a disaster event, when are GTS services available?*
A: Our services are available after 24 hours of inability to access your nVision environment.

Technical FAQ's

Q: ***How long does it take to setup the Granite Tech Solutions (GTS) Backup Agent –FM Edition on our server?***
A: Under normal conditions, and assuming that the system requirements have been reviewed before the installation, this process should take less than 30 minutes when performed by a reasonably skilled network administrator. Please make sure to see the system requirements for the backup agent proceeding with installation steps.

Q: ***What security measures are employed with the Remote Backup Service to keep our data secure?***
A: We have worked carefully and diligently to put together a service that employs multi-layered security measures. In practice, layered security is proven to be the best data security scheme.

- Our primary backup server at the Lansing, MI data center is configured with daily scans of Rootkits and Trojans, Antivirus, a software firewall, brute-force protection, TCP/IP stack protection and other security measures. Additionally, server hardening has been performed for certain key system and third party software on the server. The server runs scheduled daily checks for automatic security updates. Server security patch maintenance is reviewed on a regular schedule. This datacenter is a N+1 facility incorporating the following infrastructure: 2500 kVA utility power feed, Multiple Powerware 9315 500 kVA UPS units, Multiple Kohler 1250 kVA Diesel Generators, Multiple Liebert 20 and 22 Ton Upflow AC Units, Multiple closed circuit tv security cameras, covering all entrances and datacenter space, Site entrance controlled by electronic perimeter access card system, Site remotely monitored by 3rd party security company.

- Our secondary backup server at our Remote Disaster Recovery Center is configured with daily scans of Rootkits and Trojans, Antivirus, a software firewall, brute-force protection, TCP/IP stack protection and other security measures. The server runs scheduled checks for security updates and notifies our staff of recommended/required patches and updates. The server is also configured behind a network-level hardware firewall. Server security patch maintenance is performed on a regular schedule. Our Remote Disaster recovery Center features: Climate-controlled; Redundant Internet connectivity through Verizon FiOS and Optimum Online; 33HP 17.5 KW Generac gas generator backup; ADT Security system with fire and break-in monitoring, entry logging and cellular dial-out fail-safe option; Security cameras with DVR recording.

- ONLY authorized staff is provided access to the servers. All staff with data access is required to have an active Non-Disclosure agreement with GTS.

- Our backup agent is an executable and is encoded so that any sensitive configuration details cannot be viewed or tampered with.

- Backup files are encrypted using 256 bit AES encryption, are password protected and are stored in zip format. The files are basically useless unless someone has access to: a) The encryption key/password b) A valid FM installation c) Your FM login credentials d) A valid Progress installation

Q: ***How is our data stored and what levels of redundancy are in place?***
A: We have implemented a multi-layered approach to protect your data. In practice, a multi-layered storage scheme is proven to be the best data storage plan.

- Our primary backup server at the Lansing, MI data center is configured with RAID redundancy and a separate backup drive for storing server backups. This server is synched to our backup server at our Remote Disaster Recovery Center hourly.
- Our secondary backup server at our Remote Disaster Recovery Center is configured with a separate backup drive for storing server backups.
- Backup files are monitored for size using known-good client restore request points as benchmarks for backup file size.
- Random restores are performed by Granite Tech Solutions at the Remote Disaster Recovery Center on a periodic basis using your most recent backup files. This allows us to do a simple check that your backup file is a valid FM data archive. Granite Tech cannot validate your data as per contractual terms, login access restrictions and privacy concerns.
- Granite Tech Solutions recommends, as part of the Master Services Agreement, that you request a verification restore (non-disaster situation) to our Remote Disaster Recovery Center AT LEAST once every 3 months. This will allow you to perform a verification of your FM data via secure remote access.

Q: ***How is remote access session for our nVision data verification secured?***
A: We use LogMeIn® for remote access sessions. We are confident and satisfied with the security measures employed by LogMeIn®.

- From the service provider's website, "…whether you're concerned about general corporate governance, growing local and federal legislation, or personal privacy, LogMeIn®'s active defense security protocols help you and your organization adhere to security guidelines.
    - Layered Security Measures: Authorization of target resource to users, Authorization of users to gateway, Authorization of gateway to host, Authorization of host to gateway, 128-to-256 bit SSL end-to-end data encryption, SSL/TLS intrusion detection, IP address filtering, Denial of service filtering, IP address lockout, Authentication and authorization of users to the host, Authentication and authorization of users within the host, Detailed auditing and logging including remote control video recording, RSA SecurID support…"