



## White Paper eTapestry Application Security



### **Executive Summary**

***The privacy and security of donor data is critical to all nonprofit organizations. eTapestry understands the importance of security and the responsibility that comes with hosting an organization's data. This white paper looks at the different security issues and how eTapestry addresses them.***

*Several security issues must be addressed when securing critical business processes, whether the application is on the Internet or residing within a local network. Threats to business processing and data can be in the form of natural disasters or equipment failure or a more malicious form such as the result of a planned attack on the network or application data. There are a number of points of vulnerability that must be bolstered with a comprehensive security policy that incorporates the latest technologies in encryption, redundancy, intrusion detection, access control, auditing, authentication and network management.*

*eTapestry is committed to providing legendary service and diligence in meeting your concerns about data integrity and application availability. To this end, eTapestry has formed a strategic partnership with OneCall Internet to provide managed web hosting. OneCall brings a reputation for Internet expertise and Internet performance that is unrivaled in the industry today.*

### **The Challenges of Securing an Application**

The keys to any successful security policy are a combination of technology and people dedicated to providing a level of service that reflects a serious commitment to the responsibility of hosting an enterprise application and its data. A security policy must be in place for any critical business application, whether running on an internal, self-managed network, or using a hosted web application.

Issues of data security, accessibility, redundancy, and disaster recovery must be examined and addressed. Unfortunately, many of these issues are overlooked when systems are installed and managed locally on internal hardware. A false sense of security often exists with an internally run application resulting in software that is susceptible to any number of security and disaster situations. This can also be the case when organizations lack the resources – in equipment, money, and expertise - to properly implement a security policy. eTapestry's investment, expertise, and resources are unparalleled when compared to the alternative of a self-managed fundraising application.

### **Site protection**

OneCall data centers are physically secured server facilities designed to keep your corporate information safe. Facilities have keycard entry, palm scanners, video surveillance and are staffed by technical support people 24 hours a day, 7 days a week. The physical server is encased in a locked cabinet that has access restricted to only those authorized employees with a need to administer the physical machine.

### **Catastrophic Event & Equipment Failures**

9/11 revealed the devastation that can be caused by a single, malicious event. However, threats to an enterprise application and data need not be of malicious intent, but can stem from nature. A flood, fire, or earthquake can be devastating in the damage it can inflict on facilities and equipment. eTapestry is committed to providing backup and disaster recovery options to ensure maximum availability and integrity of the application data. **(see: Disaster Recovery FAQ's)**

OneCall provides a fully redundant network architecture with high-speed connections. Uninterruptible power supplies backed up by diesel generators at data centers ensure that power is not interrupted. The application architecture is such that processing can be redirected to other available servers in the event of a server failure.



Furthermore, the use of Java as the server application language ensures full portability to any type of machine.

eTapestry provides daily incremental file system backups, with a full disk backup weekly. (**see: Data Backup Plan**) Database backups are rotated offsite as added means of recovery should it be needed. Production servers have mirrored drive, multiple power/cooling modules and peripheral power supplies. CPU, memory, and I/O boards are all hot swappable.

On call support staff are available 24 hours a day, 7 days a week, 365 days a year to ensure any service problems are handled promptly.

eTapestry has a comprehensive disaster recovery plan in place should our primary physical site become inoperable.

### **Continuation of Service Plans**

A critical area to consider is the continued operation of any application and the accessibility of data should the business enterprise cease to operate. eTapestry customers are always 100% owners of their data. Data downloads are available at any time in a standard format usable with MS Excel or MS Access. This process allows organizations to maintain a local, usable backup of their data. The eTapestry software code is escrowed and a sophisticated continuation plan is in place should anything happen to eTapestry.

### **Over the Wire Transmission of Data**

One of the key areas to address with an Internet application is the simple transmission of data between the host server and the client workstation. The Internet works by sending information from computer to computer until the information reaches its destination. When data is sent from Point A to Point B, every computer in between these points has an opportunity to look at what is being sent. eTapestry employs a Server Digital Certificate and the Secure Sockets Layer (SSL) Protocol to encrypt all data traffic between our server and the client PC. Furthermore, SSL also protects the contents of messages exchanged between our Internet server and the client PC from being altered en route.



Revolutionizing the Charity World via Technology and Service

SSL technology is the standard used by online banking, stock brokerages, and retailers for securing their online transactions.

### **Intrusions**

Intrusions usually take one of two forms. One form can be an attempt to gain unauthorized access to data or the application. Another form can be an attempt to deny service to other users by tying up server resources or disabling the server.

*Unauthorized Access* - Authentication via username and password provides assurance that a client requesting information is the entity it claims to be.

Access Control settings limit the functionality available and types of information that users can access after being identified as an authorized user on the system.

Database activity logs record all transaction activity by user. This data can be used for accountability purposes and can be reviewed at any time by the system administrator.

*Denial of Service* – Monitoring of the eTapestry application and the hosting equipment is performed 24 hours per day. This, combined with the latest technologies in detecting and thwarting denial of service attacks insures you will have uninterrupted service.

### **Conclusion**

Critical examination of application security should be made for both internal operations and externally hosted applications. eTapestry is committed to earning client trust and keeping that trust by our implementation of technology and by our staff's integrity, diligence, and expertise as well as our strategic partnership with OneCall Internet to provide a robust and scalable hosting solution.

eTapestry provides web-based fundraising software to nonprofit organizations of all types and sizes around the world. The highest levels of product innovation, data security, and customer service are hallmarks of eTapestry. For more information, contact The Beracha Foundation at:

**877-423-7224**

**513-899-3769 (fax)**

**Solutions@Beracha.org**

**www.Beracha.org**



## Disaster Recovery FAQ's



eTapestry's role as an application service provider depends on its ability to deliver a reliable service from an application performance standpoint as well as providing mechanisms for graceful recovery in the event of system or data problems. Our partnership with OneCall Internet provides a robust and scalable web hosting environment that leverages the strengths of one of the industry leaders. OneCall provides value in the areas of qualified technical personnel, leading technology, 24x7 monitoring, and secure network infrastructures.

The following cases are meant to illustrate the procedures in place to ensure maximum application uptime and data integrity.

### **In the event of an isolated hardware failure on an eTapestry server, what is the procedure to affect a specific repair, such as replacing a hard drive?**

Because the software architecture of eTapestry has built in redundancies that eliminate a single point of failure, the impact to the end user would be minimal. However, should a hardware failure occur, an eTapestry technician will be at the server in minutes and the problem would be treated as a Severity 1 problem that justifies immediate management attention and dedicated resources in an effort to resolve the problem as soon as possible. Redundant disks remove the possibility that a single drive failure will interrupt service, however should there be an issue, eTapestry has service contracts on hardware with Sun Microsystems to provide for onsite technical service within 4 hours. In the unlikely event of multiple hard drive failures that necessitate a restore from backup, the maximum amount of data lost is limited to transactions entered since the previous night's backup.

### **What happens if the eTapestry database is corrupted?**

Since each eTapestry client is assigned its own database, a problem with one client database does not affect the ability of other clients to get to their data. eTapestry will try to diagnose the cause of the problem and repair the data as needed.

In the rare case where a database cannot be repaired programmatically, we will restore the database to the previous point in time where the corruption was not present. To date, in working with over 4000 organizations, there has not been a single instance requiring a database to be restored.

### **In the event the eTapestry server is physically damaged beyond repair, what are the steps for installing a new server?**

Since the eTapestry application is operating on multiple, redundant servers, a server outage that would disrupt customer work is unlikely. Should a server need to be replaced, eTapestry would treat this situation as a Severity 1 problem that justifies immediate management attention and dedicated resources in an effort to resolve the problem as soon as possible. A backup server would be installed in the place of the damaged machine, or if appropriate, a new server would be provisioned and installed by eTapestry.

### **What is the procedure in the event of a massive failure or catastrophic event at the OneCall data center? Is there a provision for relocating to another data center? What is the timetable for such a relocation?**

The OneCall data center is a highly secure facility with state of the art protection against intrusion, power disruption, and fire. In addition, it has been built to withstand up to an F4 level tornado making it very safe against natural disaster. Should a data center problem arise, it would be treated as a Severity 0 problem justifying immediate management attention and dedicated resources. Servers would be relocated to an alternate data center. This would require a DNS change that would have to propagate to the various Internet Domain Servers in order for clients to access the relocated server. Relocation and reinstallation of all systems would require 24-48 hours of downtime. Offsite backups would be used to minimize any loss of data. A communication plan would be implemented immediately to notify all customers of the process and status.



## Data Backup Plan

An organization's database of donors, prospects, and their gift and contact information is one of the most important assets they have. A comprehensive data backup plan is critical - whether you are managing your database internally, or utilizing a hosted application. At eTapestry we are diligent and dedicated to protecting and maintaining the security of our customer's data. The following information highlights just one aspect of our overall security – but one that is critical to our customer.

### **Purpose:**

To insure that we maintain a process of data backups and storage of production server data that protects our customers' data in the event of catastrophic circumstances. The plan incorporates several levels of redundancy that virtually eliminates potential loss of data while providing for rapid recovery if needed.

### **Overview:**

Production server data (incremental backup) is backed up onto tapes daily with one copy kept at the hosting center and the other stored offsite. In addition 2 full backups are made each week off the production server. One is kept at the hosting center managed by OneCall Internet, and the other is picked up and stored off-site at a local bank safe deposit box. Also weekly, a tape backup is made off the eTapestry internal server (which stores a local backup of the production server) and is stored in a fireproof safe kept at eTapestry headquarters.

### **Activities:**

#### **Daily**

- 2 Incremental tape backups made of Production server – 1 kept at OneCall Internet, the other taken off site to safe deposit box

#### **Weekly**

- 2 full system backups made of Production server – 1 kept at OneCall Internet, the other taken off site to safe deposit box
- Tape backup made off the local eTapestry server and stored in a fireproof safe kept at eTapestry offices

#### **Monthly**

- Backup tapes from both units tested to insure the restore procedure is working properly
- Full backup copy of Production server made and stored in bank safe deposit for period of one year
- Full backup copy of internal server made and stored internally in fireproof safe for period of one year

#### **Quarterly**

- Firedrill performed that would simulate Production server failure and the loading onto an alternative/temporary server

These procedures are constantly being reviewed, revised, and updated in an effort to continually provide the best security and protection for our customers.

### **For Sales Support:**

**877-4BERACHA (423-7224) Ext. 2**

[Solutions@Beracha.org](mailto:Solutions@Beracha.org)

[www.Beracha.org](http://www.Beracha.org)