DONORPRO™
Informational Series

Part 3: Database Integrity and Database Security

January 2010

By Gina Davis, DonorPro Implementation Specialist, TowerCare Technologies, Inc.

The integrity and security of your database is absolutely essential. Security means keeping your data safe. Integrity means keeping your data accurate, consistent and valid. This article will explore database integrity and security so that you will be armed with enough information to effectively protect your data.

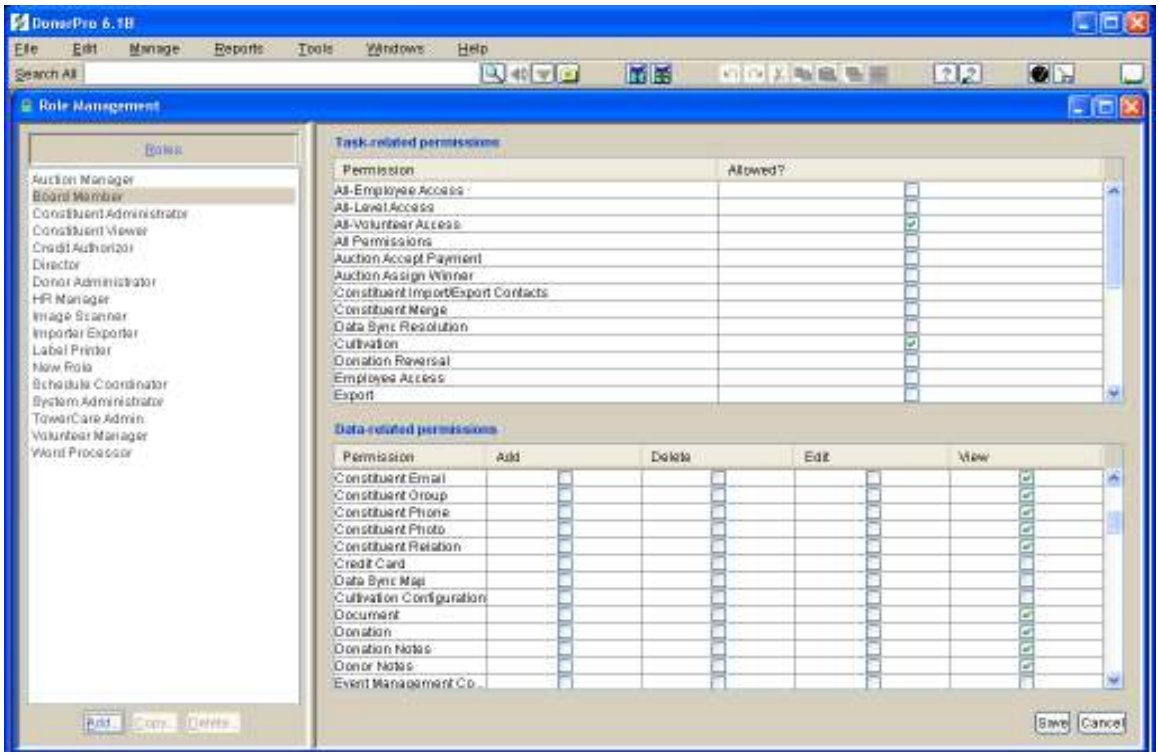
Let's start with data integrity. Having data integrity ensures that all data within the database adheres to the guidelines or structure of the database. For example, each record in your database should have a unique identifier, such as a specific constituent number. It is also important that if you delete the main constituent record, then information related to that record is also deleted. If related information is not removed from your database, then you end up with orphan records, such as donations with no donor listed. The rule that governs unique identifiers and prevention of orphan records is called referential integrity. If there is no referential integrity in your database then users can enter any data they want, sometimes without regard to entering a complete or useful record. When considering a database, verify that there is some level of referential integrity.

Data integrity also refers to data being accurate and consistent. As with referential integrity, to achieve accuracy and consistency, certain rules must be built into your database. For example, if there is a date field, you don't want users to be able to enter random text. Data entry in that field should be limited to dates only. It is also advisable to establish best practices for regularly cleaning your database. Reviewing your data by running a query against the database and then checking the output is one of the most common ways to find data inconsistencies.

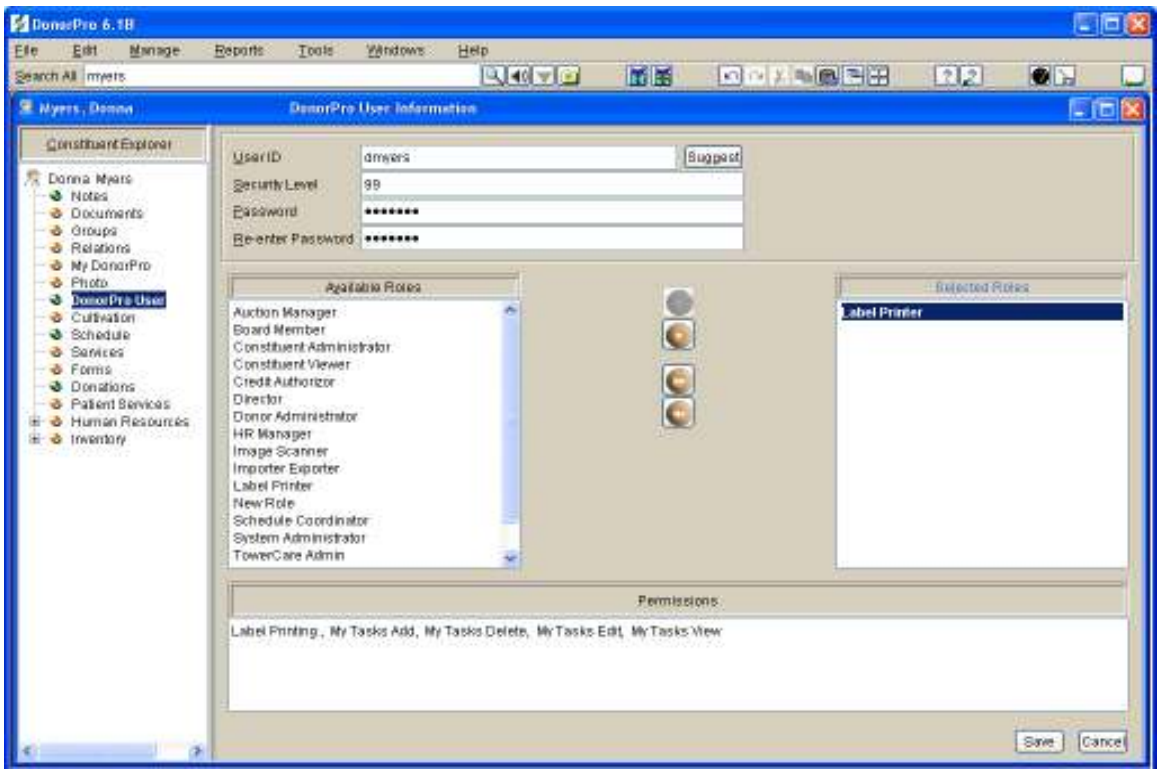
Robust database security is vital for protecting information about your constituency. This security should prevent unauthorized access to your database. It should also prevent your data from being altered or deleted by users without the appropriate permissions. You need to protect your data not only from hackers, but also by not allowing database users access to more areas of your database than they need in order to do their jobs. Safeguards must be in place before you ever begin using your database. Here is a checklist of items to help you keep your data secure.

- ✓ **Data Encryption**
  - This refers to data being made unreadable by anyone who does not have the appropriate decryption key.

- ✓ **Firewall**
  - A firewall is a device or software system that is used to block unauthorized access to a computer, computer network, or intranet.
- ✓ **Anti-virus software**
  - This type of software helps to prevent, detect, and remove malicious programs or code from your computer. It may also help to remove adware (software that automatically plays or downloads advertisements) and spyware (code that installs itself on a computer and collects information about the user without their knowledge).
- ✓ **Database backups**
  - A backup is a copy of your database. This should be done often and at regular intervals, at least on a nightly basis. In the event of equipment failure or some type of data corruption, you should be able to recover your undamaged database to the point of the most recent backup.
  - Remember to keep your data backup files in a safe and secure location. It is best practice to store your backups in a separate location from the actual data source to protect from unforeseen events like theft, fire, or flood.
- ✓ **Password protection**
  - It is important that you and your staff create strong passwords for your computers and for your database software. Make sure to choose a database that requires a secure log in for use. Strong passwords are ones that are not easy to guess and should include special characters such as an exclamation point or pound sign, numbers, and a mix of both upper and lower case letters.
  - The password should be required not only when you turn on your computer, but also when your computer remains inactive for a specified length of time. This is sometimes referred to a screen saver password.
  - Your database software should keep track of failed login attempts and readily provide you with these logs so that you can determine if unauthorized personnel are trying to access your data.
- ✓ **Log off**
  - When you leave the office, never stay logged on to your computer. Anytime that you are going to be away from your computer, at a minimum, you should log off from your database software. When you leave your office, you should either shut down or log off of your computer so that others cannot access anything on your computer or network using your log in credentials.
- ✓ **Limit access**
  - All users should have their own unique user id and password to access the database. A good database will allow you to see an audit trail of what users are doing in the database.
  - When an employee leaves their job, immediately revoke all access to your database and computer networks in your organization. Remember too that you will also need to change any passwords that were shared with that employee.
  - Access to database functions and particular data should be restricted to only what the user needs to do their job. Look for a database that provides both role and rights based security.



From this DonorPro screen, the administrator defines specific roles within the organization and then based on the role, selects the permitted tasks for that role. For each role, the administrator also defines specific data related permissions which determine what a person with that role can see in the database and what data he/ she can edit, add, or delete.



For example, for a volunteer who is coordinating a direct mailing, you might assign the role of "Label Printer." This screen shows that the "Label Printer" is limited to view only a small subset of data within DonorPro and is also limited to performing only a few select tasks in DonorPro like printing labels.

- ✓ **PCI compliance**
  - The Payment Card Industry Data Security Standard (PCI DSS) is to not store complete credit card numbers. Sensitive data must be encrypted and access to information must be closely controlled. This is to protect you from liability and to protect your donor's confidential information. Make sure your database software is PCI compliant.
- ✓ **Physical security**
  - You would not leave your purse or your wallet out in the open or on the seat of your car where someone just passing by could see it and take it. The same should apply to your laptop. Physical security of your computer is just as important as digital security.
  - If your database software is web-based or provided under a SaaS model (Software as a Service) which is often referred to as an ASP (Application Service Provider) implementation , it is critical to verify that your vendor's datacenter is highly secure since this is where your actual database/data will reside. The datacenter itself should be in a highly secure building with 24 hour monitors. Access to the datacenter should be granted only to vendor's key employees. No one should be able to access the datacenter without appropriate photo identification.
- **Logical Security**
  - If your database vendor is hosting your nonprofit's database, make sure the vendor has taken all necessary logical security precautions including internal and external firewalls. Is access to the servers that are storing your data done through non-standard ports to reduce break-in attempts? All connections to the server housing your data should use a secure and encrypted protocol such as HTTPS.

Without data integrity you will not have quality data. Quality data is essential for building support for your mission. With quality data, you can build a development program that identifies persons and organizations who care about your mission and address the needs of these prospects when making an "ask." If you do not have secure data then you cannot count on your data to be available or to be accurate. Integrity and security go together in protecting your data both internally and externally.

I hope you found this information to be helpful and informative. Please look for the fourth article in the *Database Management for Nonprofits Series* which will be available for download in March 2010at www.towercare.com.

If you are in the market for database software, check out DonorPro. DonorPro is easy to use and affordable database software built by nonprofit professionals. Call toll free 866-935-8281 or visit our online DonorPro Product Tours at www.towercare.com/content/product-tours.