**YuniquePLM Backup Plan**

June 2010 (v3.x)

# Protect your Users

## Back up your Databases

At Gerber Technology, we dedicate ourselves to providing our customers a quality product. Ensuring that software glitches, hardware failures, or vindictive acts do not compromise the creative work your users do is critical. The single most important thing that you can do is to backup your database. The following questions will help determine how frequently your database(s) should be backed up.

1. How much data/work are you willing to lose?  
   Let us assume putting a line in requires the creation of 160 folders during a 40-hour workweek or 4 folders per hour. That means you will lose 4 folders per hour of down time.
2. What types of resources are available to perform database backups?
3. How stable is your environment? Do you have network outages?

# Protect your Data

## Check your Database for reliability

Just because a database backup has recently been performed does not mean that you can restore your database. The database backup needs to be:

1. Checked for errors. ( DBCC CHECKDB WITH NO\_INFOMSGS)
2. Restored during a testing phase to ensure that the backup plan works. You do not want to find out during an emergency that your database backup cannot be restored.

Once you have restored a database (at least once) and are checking for errors, your investment in people, time and money are protected.

# Protect your Investment

## Backup and recovery for SQL Server

SQL Server supports 3 different types of backups:

1. Full database backups: All of the data in your database is saved. This is effectively a database snapshot.
2. Differential database backups: Saves off all of the data that has changed since the last time a full database backup occurred. If your last full database backup was at 1:00 A.M. and your most recent differential database backup occurred at 3:00 A.M., it would have recorded all changes in the database between 1:00 A.M. and 3 A.M.
3. Transaction log backups: Saves off on an individual basis all changes/transactions that have occurred in the database.

Gerber recommends to our customers the following information:

1. Backup your database regularly (with a full database backup) every night.
2. Perform a transaction log backup at least once per evening and preferably every 8 hours. As long as the log file gets backed up your valuable work is protected.
3. Backup the ‘master’ database after an upgrade.

In the event of total disaster (i.e. disk crash) your worst data loss under the above mentioned scenario is 8 hours work lost. However, if Raid 5 is being used your window of time data loss is much less than 8 hours.

To restore your database from the full database backup and transaction log backup mentioned above, you will need to:

1. Restore the most recent full database backup.
2. Apply all transaction logs created after the last full database backup was created.

## Checking your SQL Server Database for errors

There are several routines that are supplied by the SQL Server database vendor that help to check a database for errors. They are all part of the DBCC (Database Consistency Check) command. Each of the commands mentioned below should be scheduled on a periodic basis with the results checked for errors.

1. DBCC CHECKDB - Checks the allocation and structural integrity of all the objects in the specified database.
2. DBCC CHECKALLOC - Checks the allocation and use of all pages in the specified database.

Each of these routines is described in detail in the SQLServer Transact SQL (T-SQL) manual.

# Protect Your Investment

**❖ Note:** Companies typically use 3rd party backup software to back up their databases. Always remember to purchase the plug-ins that allows a database backup to occur while it is online. Otherwise, you may find that out that your database backups are worthless because the files were locked and they did not actually get saved off to tape or disk.

## Image files

YuniquePLM does not store any images within the database. All images are stored on a file server. The RDBMS system backup does not save the images stored on the NT file system to tape/disk. You need to backup these separately.

Each time that you perform a full database backup, differential database backup, or transaction log backup you should be performing an incremental or full backup of your image files on your Windows system. This incremental backup of your image files assumes that a backup of the image files currently exist..

## Server

Please remember to backup your server. If you do not maintain a relatively current backup of your system along with any necessary emergency boot disks you may have to install your server, RDBMS and the YuniquePLM system from scratch. It takes significantly more time to recover from a server failure if you need to re-install than if you just reload from an archive.

# Summary

Create 1 or more maintenance plans to accomplish the following:

1. Rebuild the table indexes of the YuniquePLM database at least monthly. Increase frequency depending on transactional volume.
2. Reorganize indexes and update statistics at least weekly. Increase frequency depending on transactional volume.
3. Backup the transaction log of the YuniquePLM database on a scheduled periodic basis. Depending on load this could be anywhere from every 15 minutes to every 8 hours. This depends on corporate risk tolerance.
4. Shrink the transaction log of the YuniquePLM and Reportserver databases. This will eliminate log creep. Backing up the transactions logs will not actually shrink the transaction log file size.
5. Perform scheduled full database backups of the YuniquePLM and ReportServer databases. This should be performed at least once a day.
6. Move/Delete old transaction log backups that are more than x days old (x is infrastructure based). Never delete the log backups if they have not been saved to offline storage.
7. Move/Delete the full database backups for the YuniquePLM and ReportServer databases. Do not delete old backups if they have not been saved to offline storage. Just like transaction log backups the frequency of cleanup is typically tied to corporate infrastructure (AKA disaster recovery policy, and disk storage availability). It is always easier and faster to restore from an online backup than it is to from tape/offline storage.