Jackson Hole Mountain Resort

<table>
<thead>
<tr>
<th>Backup Policy</th>
<th>Created: 10/20/2011</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section of: Corporate Security Policies</td>
<td>Target Audience: Technical</td>
</tr>
<tr>
<td>CONFIDENTIAL</td>
<td>Page 1 of 5</td>
</tr>
</tbody>
</table>

Jackson Hole Mountain Resort is hereinafter referred to as "the company."

1.0 Overview

A backup policy is similar to an insurance policy - it provides the last line of defense against data loss and is sometimes the only way to recover from a hardware failure, data corruption, or a security incident. A backup policy is related closely to a disaster recovery policy, but since it protects against events that are relatively likely to occur, in practice it will be used more frequently than a contingency planning document. A company's backup policy is among its most important policies.

2.0 Purpose

The purpose of this policy is to provide a consistent framework to apply to the backup process. The policy will provide specific information to ensure backups are available and useful when needed - whether to simply recover a specific file or when a larger-scale recovery effort is needed.

3.0 Scope

This policy applies to all data stored on corporate systems. The policy covers such specifics as the type of data to be backed up, frequency of backups, storage of backups, retention of backups, and restoration procedures.

4.0 Policy

4.1 Identification of Critical Data

The company must identify what data is most critical to its organization. This can be done through a formal data classification process or through an informal review of information assets. Regardless of the method, critical data should be identified so that it can be given the highest priority during the backup process.

Critical SQL Server databases are:
- RTPOne on SONORA
- JHMRCustom on SONORA
- eStoreAccount on MARS
Backup Policy

Section of: Corporate Security Policies
Target Audience: Technical

CONFIDENTIAL Page 2 of 5

- Dynamics/Great Plains-JHMR on MARS
- Dynamics/Great Plains-Dynamics on MARS
- JHMRCustom on MARS
- TimeCentre (TC2KDB) on MARS
- FoodTrack on MARS
- Fleetmax on MARS
- Training on MARS
- WEBROOT on MARS
- Avalanche Lab Weather on MARS
- System databases for servers SONORA & MARS

4.2 Data to be Backed Up
A backup policy must balance the importance of the data to be backed up with the burden such backups place on the users, network resources, and the backup administrator. Data to be backed up will include:

- All data determined to be critical to company operation and/or employee job function.
- All information stored on the corporate file server(s). It is the user's responsibility to ensure any data of importance is moved to the file server.
- All information stored on network servers, which may include web servers, database servers, domain controllers, firewalls, and remote access servers, etc.

Data stored in the NetApp Storage Area Network is stored redundantly with real-time backups and periodic snapshots. This is the primary line of defense for backup of this data. In addition, disk to disk backups are performed nightly.

Non-- SQL Server data to be backed up:
- All contents of the company share (the J Drive - \jhmrcicom\dfs\company*)
- All contents of user shares (the I Drives - \jhmrcicom\dfs\user*)
  - All contents of the shares at the root of \jhmrcicom\dfs as follows: HR-Payroll
  - Payroll
  - Premiere
  - Secure
  - Secure Too
  - Techs

Note that NO USER DESKTOP DATA OR C DRIVE DATA IS BACKED UP. Users are
Backup Policy

4.3 Backup Frequency
Backup frequency is critical to successful data recovery. The company has determined that the following backup schedule will allow for sufficient data recovery in the event of an incident, while avoiding an undue burden on the users, network, and backup administrator.

All SQL backups are performed nightly.
All shared data backups are performed nightly.

4.4 Off-Site Rotation and Storage
Geographic separation from the backups must be maintained, to some degree, in order to protect from fire, flood, or other regional or large-scale catastrophes. Offsite storage must be balanced with the time required to recover the data, which must meet the company's uptime requirements. The company has determined that backup media must be rotated off-site at least once per day.

SQL backups and Shared data are streamed to a secondary backup store located in the Bridger Center each day.

4.5 Backup Storage
Storage of backups is a serious issue and one that requires careful consideration. Since backups contain critical, and often confidential, company data, precautions must be taken that are commensurate to the type of data being stored. The company has set the following guidelines for backup storage.

There are no restrictions to how and where backups can be stored when on-site. When shipped off-site, backups should be reasonably secured from theft or fire. A hardened facility (i.e., commercial backup service or safe deposit box) can be used but is not required. Online backups are allowable if the service meets the criteria specified herein.

4.6 Backup Retention
When determining the time required for backup retention, the company must determine what number of stored copies of backup-up data is sufficient to effectively mitigate risk while preserving required data. The company has determined that the following will meet all requirements (note that the backup retention policy must confirm to the company's data retention
Jackson Hole Mountain Resort

<table>
<thead>
<tr>
<th>Backup Policy</th>
<th>Created: 10/20/2011</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section of: Corporate Security Policies</td>
<td>Target Audience: Technical</td>
</tr>
<tr>
<td>CONFIDENTIAL</td>
<td>Page 4 of 5</td>
</tr>
</tbody>
</table>

policy and any industry regulations, if applicable):

4.7 **Restoration Procedures & Documentation**
The data restoration procedures must be tested and documented. Documentation should include exactly who is responsible for the restore, how it is performed, under what circumstances it is to be performed, and how long it should take from request to restoration. It is extremely important that the procedures are clear and concise such that they are not A) misinterpreted by readers other than the backup administrator, and B) confusing during a time of crisis.

4.8 **Restoration Testing**
Since a backup policy does no good if the restoration process fails it is important to periodically test the restore procedures to eliminate potential problems.

Backup restores must be tested when any change is made that may affect the backup system, as well as once every month.

4.9 **Expiration of Backup Media**
Certain types of backup media, such as magnetic tapes, have a limited functional lifespan. After a certain time in service the media can no longer be considered dependable. When backup media is put into service the date must be recorded on the media. The media must then be retired from service after its time in use exceeds manufacturer specifications.

4.10 **Applicability of Other Policies**
This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 **Enforcement**

This policy will be enforced by the IT Director and/or CFO. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.
6.0 Definitions

Backup  To copy data to a second location, solely for the purpose of safe keeping of that data.

Backup Media  Any storage devices that are used to maintain data for backup purposes. These are often magnetic tapes, CDs, DVDs, or hard drives.

Full Backup  A backup that makes a complete copy of the target data.

Incremental Backup  A backup that only backs up files that have changed in a designated time period, typically since the last backup was run.

Restoration  The process of restoring the data from its backup-up state to its normal state so that it can be used and accessed in a regular manner.

Recovery  The process of thinking restored data ready for use by systems, applications, and users.

7.0 Revision History

Revision 1.0, 10/20/2011
Revision 1.1, 11/8/2011