Jackson Hole Mountain Resort

<table>
<thead>
<tr>
<th>Encryption 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 3</td>
</tr>
</tbody>
</table>

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

1.0 Overview

Encryption, also known as cryptography, can be used to secure data while it is stored or being transmitted. It is a powerful tool when applied and managed correctly. As the amount of data the company must store digitally increases, the use of encryption must be defined and consistently implemented in order ensure that the security potential of this technology is realized.

2.0 Purpose

The purpose of this policy is to outline the company’s standards for use of encryption technology so that it is used securely and managed appropriately. Many policies touch on encryption of data so this policy does not cover what data is to be encrypted, but rather how encryption is to be implemented and controlled.

3.0 Scope

This policy covers all data stored on or transmitted across corporate systems.

4.0 Policy

4.1 Applicability of Encryption
1. Data while stored. This includes any data located on company-owned or company-provided systems, devices, media, etc. Examples of encryption options for stored data include:

- All "Customer Data" as defined by the PCI – DSS 2.0 standard is encrypted in all company SQL Server databases at the highest level.

- As this data is strongly encrypted in the databases, no further database backup encryption is utilized.

2. Data while transmitted. All "Customer Data" as defined by the PCI – DSS 2.0 standard is fully encrypted in the company's network at all times.
4.2 Encryption Key Management
Key management is critical to the success of an implementation of encryption technology. The following guidelines apply to the company's encryption keys and key management:

- Management of keys must ensure that data is available for decryption when needed
- SQL Server encryption keys are stored in the possession of the IT director and other members of the IT team.

4.3 Acceptable Encryption Algorithms
Only the strongest types of generally-accepted, non-proprietary encryption algorithms are allowed, such as AES or 3DES. Acceptable algorithms should be reevaluated as encryption technology changes.

Use of proprietary encryption is specifically forbidden since it has not been subjected to public inspection and its security cannot be assured.

4.4 Legal Use
Some governments have regulations applying to the use and import/export of encryption technology. The company must conform with encryption regulations of the local or applicable government.

The company specifically forbids the use of encryption to hide illegal, immoral, or unethical acts. Anyone doing so is in violation of this policy and will face immediate consequences per the Enforcement section of this document.

4.5 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 Senior Team. 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
Jackson Hole Mountain Resort

<table>
<thead>
<tr>
<th>Encryption 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 3 of 3</td>
</tr>
</tbody>
</table>

property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

6.0 Definitions

**Encryption** The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.

**Encryption Key** An alphanumeric series of characters that enables data to be encrypted and decrypted.

**Mobile Storage Media** A data storage device that utilizes flash memory to store data. Often called a USB drive, flash drive, or thumb drive.

**Password** A sequence of characters that is used to authenticate a user to a file, computer, or network. Also known as a passphrase or passcode.

**Remote Access** The act of communicating with a computer or network from an off-site location. Often performed by home-based or traveling users to access documents, email, or other resources at a main site.

**Remote Desktop Access** Remote control software that allows users to connect to, interact with, and control a computer over the Internet just as if they were sitting in front of that computer.

**Virtual Private Network (VPN)** A secure network implemented over an insecure medium, created by using encrypted tunnels for communication between endpoints.

**Whole Disk Encryption** A method of encryption that encrypts all data on a particular drive or volume, including swap space and temporary files.

7.0 Revision History

Revision 1.0, 10/20/2011
Revision 1.1, 10/30/2011