# Jackson Hole Mountain Resort

| VPN Policy | Created: 10/20/2011 |
|---|---|
| Section of: Corporate Security Policies | Target Audience: Technical |
| CONFIDENTIAL | Page 1 of 3 |

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

## 1.0 Overview

A Virtual Private Network, or VPN, provides a method to communicate with remote sites securely over a public medium, such as the Internet. A site-to-site VPN is a dependable and inexpensive substitute for a point-to-point Wide Area Network (WAN). Site-to-site VPNs can be used to connect the LAN to a number of different types of networks: branch or home offices, vendors, partners, customers, etc. As with any external access, these connections need to be carefully controlled through a policy.

## 2.0 Purpose

This policy details the company's standards for site-to-site VPNs. The purpose of this policy is to specify the security standards required for such access, ensuring the integrity of data transmitted and received, and securing the VPN pathways into the network.

## 3.0 Scope

The scope of this policy covers all site-to-site VPNs that are a part of the company's infrastructure, including both sites requiring access to the company's network (inbound) and sites where the company connects to external resources (outbound). Note that remote access VPNs are covered under a separate Remote Access Policy.

## 4.0 Policy

### 4.1 Encryption

Site-to-site VPNs must utilize strong encryption to protect data during transmission. Encryption algorithms must meet or exceed current minimum industry standards, such as Triple DES or AES.

### 4.2 Authentication

Site-to-site VPNs must utilize a strong password, pre-shared key, certificate, or other means of authentication to verify the identity the remote entity. The strongest authentication method available must be used, which can vary from product-to-product.

## 4.3 Implementation

When site-to-site VPNs are implemented, they must adhere to the policy of least access, providing access limited to only what is required for business purposes. This must be enforced with a firewall or other access control that has the ability to limit access only to the ports and IP addresses required for business purposes.

## 4.4 Management

The company should manage its own VPN gateways, meaning that a third party must not provide and manage both sides of the site-to-site VPN, unless this arrangement is covered under an outsourcing agreement. If an existing VPN is to be changed, the changes must only be performed with the approval of the IT Director.

## 4.5 Logging and Monitoring

Depending on the nature of the site-to-site VPN, the IT Director will use his or her discretion as to whether additional logging and monitoring is warranted. As an example, a site-to-site VPN to a third party would likely require additional scrutiny but a VPN to a branch office of the company would likely not be subject to additional logging or monitoring.

## 4.6 Encryption Keys

Site-to-site VPNs are created with pre-shared keys. The security of these keys is critical to the security of the VPN, and by extension, the network. Encryption keys should be changed periodically.

If certificates are used instead of pre-shared keys, the certificates should expire and be re-generated after three years.

## 4.7 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 property (physical or intellectual) are suspected, the company may report such activities to the

applicable authorities.

# 6.0 Definitions

**Certificate** Also called a "Digital Certificate." A file that confirms the identity of an entity, such as a company or person. Often used in VPN and encryption management to establish trust of the remote entity.

**Demilitarized Zone (DMZ)** A perimeter network, typically inside the firewall but external to the private or protected network, where publicly-accessible machines are located. A DMZ allows higher-risk machines to be segmented from the internal network while still providing security controls.

**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.

**Remote Access VPN** A VPN implementation at the individual user level. Used to provide remote and traveling users secure network access.

**Site-to-Site VPN** A VPN implemented between two static sites, often different locations of a business.

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

# 7.0 Revision History

Revision 1.0, 10/20/2011
Revision 1.1, 10/31/2011