|  |  |  |
| --- | --- | --- |
| **SMTAFE Information Security Policy** | | |
| ***Audience:*** | SMTAFE Employees and Management | |
| ***Approval Authority:*** | CEO | |
| ***Contact:*** | mail to: security@smtafe.gov.au | |
| ***Status:*** | Proposed: | November 6, 2018 |
| Last updated: | TBA |

##### SMTAFE

##### Information Technology Security Plan

November 6, 2018

Contents

[Introduction 3](#_Toc528528521)

[Information Technology Security Safeguards 4](#_Toc528528522)

[Physical Security 4](#_Toc528528523)

[Personnel Security 5](#_Toc528528524)

[Data Communications Security 5](#_Toc528528525)

[Phone System Security 5](#_Toc528528526)

[System Access Security 5](#_Toc528528527)

[Authentication 5](#_Toc528528528)

[Passwords Policy 6](#_Toc528528529)

[Data Classification 6](#_Toc528528530)

[Access Rights 7](#_Toc528528531)

[Legal Safeguards 7](#_Toc528528532)

[Licensing 7](#_Toc528528533)

[Privacy 7](#_Toc528528534)

[Legal Disclaimers 7](#_Toc528528535)

[Logon Banner: 7](#_Toc528528536)

[Web Disclaimer 8](#_Toc528528537)

[Network Usage Policy 8](#_Toc528528538)

[Ensuring System Integrity 8](#_Toc528528539)

[Virus Protection 8](#_Toc528528540)

[Redundancy and Backups\*\* 8](#_Toc528528541)

[Security Verification 9](#_Toc528528542)

[Security Logs 9](#_Toc528528543)

[Security Verification Team 9](#_Toc528528544)

[Handling Non-compliance 10](#_Toc528528545)

[Security Awareness and Training 10](#_Toc528528546)

[Appendix A. Local Windows Client for Netware Configuration Utility Settings 11](#_Toc528528547)

[Appendix B. Standard Windows 10™ Security Settings 11](#_Toc528528548)

[Appendix C. Firewall Policy 12](#_Toc528528549)

[Appendix D. List of Staff who have access to the IT Infrastructure Documentation. 12](#_Toc528528550)

# Introduction

TiO2 Mineral Consultants Pty Ltd referred to throughout this document as “SMTAFE”. The objectives of the SMTAFE IT Security Plan are the following:

        Acquaint employees with the security procedures required to ensure protection of information technology systems at SMTAFE.

        Clarify employee responsibilities and duties with respect to the protection of information resources.

        Enable managers and other workers to make decisions about information security which are in keeping with standard policies and procedures, and which are responsive to prevailing local conditions.

        Coordinate the efforts of different groups within SMTAFE so that information resources are properly and consistently protected, regardless of their location, form, or supporting technologies.

        Provide guidance for the performance of information system security audits and reviews.

        Demonstrate management support for a strong information security program at SMTAFE.

        Establish a basis for disciplinary actions when required to protect SMTAFE information assets.

SMTAFE is taking appropriate steps to ensure its information systems are properly protected from all security threats.  All SMTAFE information systems shall be protected, regardless of storage or transmission medium.

 Three key concepts form the backbone of the security program at SMTAFE:

1. The commitment to protecting vital and confidential electronic files.

2. All information access is granted consistent with the acceptable use policy.

3.      Information security is the responsibility of all computer system users.

All security procedures in this document are written with these three concepts in mind.

**SMTAFE Network Administrator**

Network Administration Personnel who serve as primary Network Administrators. Staff serve to implement and maintain security of electronic information. They are responsible for assessing the security risks and external threats, recommending actions to minimize those risks, and conducting program reviews to assess the adequacy of internal controls, structures, and business processes to protect client and corporate information and technology resources.

The SMTAFE Network Administrators have been assigned the following responsibilities:

        Maintain and verify network and host security for all business systems.

        Develop and maintain formal security policies and procedures.

        Maintain and verify user ID and data set security databases.

        Maintain and verify users, groups and assignments in the databases.

        Verify and review Network Share Level access rights.

        Verify Local Area Network switch/router security settings.

* Collaborate with all staff and management on information security planning and maintenance.

        Develop and maintain a formal security awareness and training program.

# Information Technology Security Safeguards

This security plan requires that good management practices be followed to implement information technology security safeguards based on the SMTAFE IT Risk Assessment.  The following is a list of requirements for all information systems maintained at SMTAFE.

## Physical Security

        All network servers shall be in a locked room or secured in a locked enclosure.

        All network server rooms shall have CO2 based fire extinguishers located within the room.  Network Technicians shall be aware of the location of the closest fire alarm.  The network server room shall have a smoke detector installed in the room.

        The network server room should be monitored for temperature and humidity.

        All network servers shall be run on an uninterruptible power supply (UPS).

        An access list of personnel that are approved access to the server room or LAN/Phone closet shall be kept.  A logging system shall be set up to document any visitors to the server room or LAN/Phone closet not on the approved access list.  All visitors to the server room or LAN/Phone closet shall be escorted at all times.

        No drinking is allowed around computer equipment.

        Sensitive information shall not be stored on portable computers that are taken outside of secured areas.

        Do not leave confidential information on desks after working hours or in rooms that are un-attended.

        When dealing with confidential information, ensure that no one is watching over your shoulder.  This precaution should also be taken when typing in passwords.

        Attended operation is required when printing confidential information to an unsecured location.

## Personnel Security

Existing Federal, state law, and regulations impose significant responsibilities on employees for the security of information. Therefore, SMTAFE has instituted the following personnel security measures:

        Prospective new employees applying for positions which have access to sensitive data will be screened as to their trustworthiness in handling sensitive data.

        All individuals with access to sensitive data must be familiar with SMTAFE policies and procedures relating to sensitive data.

        Technical support personnel will be cross-trained so that procedures can be followed unaffected by the absence of any one key individual.

## Data Communications Security

A Firewall and Security Services (i.e., Firewall) shall be placed between each organization’s network and the SMTAFE wide area network (WAN) which provides SMTAFE with Internet access.

Where possible, individuals shall use only encrypted means of access information across the Internet.  Where this is not possible, individuals shall not pass sensitive business information.  Encryption methods shall use at least *128-bit encryption keys*.

Remote access to the SMTAFE network shall be strictly controlled.  A list of all modems or other connections connected to the SMTAFE network shall be kept. All dial-in and dial-out shall be accomplished using the SMTAFE network server when available in order to ensure that all network access is logged.

## Phone System Security

The phone system is meant primarily to handle the business needs of SMTAFE.  To this end, personal use of the SMTAFE phone system should not interfere with the business operations of SMTAFE. 

## System Access Security

### Authentication

The identity of each individual who accesses business information must be verified before given access to the information.  This identification process is normally performed using the user ID/password process.  The user ID determines who the user is claiming to be.  The submission of a correct password is taken to mean that the person is actually who the user ID claims them to be.

        Use of shared user ID’s shall be limited to workstations allowing only single function use (such as workstations secured so that they can only be used to browse the web).

        All users shall be forced to change their passwords every 200 days.

        SMTAFE Systems shall be set to lock out further logon attempts for at least 2 minutes after 10 failed attempts have occurred.

        A notice of last logon time and date is recorded.

### Passwords Policy

Passwords are generally obtained by 4 common methods.  Therefore, SMTAFE requires that all passwords have 4 characteristics that ensure they will not be found using one of the 4 common methods.  All passwords used at SMTAFE must be:

        Long - (Minimum 6 characters) to thwart brute force attacks

        Non-English – i.e., not in an English dictionary to thwart dictionary attacks, therefore SMTAFE requires that all passwords have at least one non-alphabetic character in the password

        Un-guess-able – not obtainable from information known about the person. This characteristic keeps an attacker from guessing the password.

        Memorable – allows the user to remember the password without writing it down.  This characteristic ensures an attacker will not find a written down password.

In addition to the 4 characteristics of individual passwords, to maintain good security individual passwords should not have any relationship to other passwords in use.  That way if an attacker obtains one password, they will not be able to gain access to other passwords maintained by the same person.  Passwords should not be accessible by anyone except by the owner of the password.  Passwords should be changed regularly.

        Passwords should not be cyclical.  When a password expires, do not name the new password as an identifiable iteration of the last password (i.e, pass1, pass2, pass3, etc.)

        Passwords used in the business should not be used on systems outside the business

        Do not share passwords with others.

        Passwords must not be stored in readable form in batch files or other locations unless sufficient security precautions are taken to ensure the security of the password.

        All vendor default passwords must be changed upon system installation.

        If a suspected disclosure of passwords has occurred, all involved passwords shall be immediately changed.

        Proof of identity is required to obtain a reset password.

        All users will be forced to change their passwords every 200 days or their accounts will be automatically disabled.

         New passwords will be issued in a state that requires immediately changing the first time the user logs on.

### Data Classification

All sensitive information shall be labeled either [confidential] or [internal use only] in the document containing the sensitive information.  At least once per quarter, the SMTAFE Network Administrators will search the SMTAFE network to ensure that confidential and internal use only documents are not accessible to the general public.

        All personal data shall be treated as confidential information.

        All storage medium shall be classified to highest level of information they may contain.

        All storage medium must be destroyed or securely wiped before disposal

### Access Rights

Once a user is authenticated, they are only given access to information necessary to complete their job function.  All data shall be controlled to limit access to individuals who need access to the information.

        Dormant user IDs shall be removed every 6 months.

        A list of access rights to network resources shall be generated and reviewed by management yearly.

## Legal Safeguards

### Licensing

        SMTAFE must have documentation proving compliance with software license agreements.  If an end user loads personal software on their PC, they must provide the SMTAFE help desk with a copy of software license and proof of purchase or a statement saying that the user has in their possession a legal license for this software.

        SMTAFE is committed to obeying intellectual property laws such as the AUS. copyright law as it relates to electronic information and copyrights.

        The SMTAFE Network Administrator will perform a periodic review of software licensing to ensure that SMTAFE complies to the software license agreements.

### Privacy

        SMTAFE shall attempt to ensure privacy of communications over its telephone and data networks.  However, it should be noted that messages sent over SMTAFE internal electronic mail systems are subject to the privacy provisions of The Telecommunications (Interception and Access) Act 1979, and therefore may legally be read by SMTAFE management and network administrators if deemed necessary to meet business and legal requirements.

        All SMTAFE information systems, consisting of the equipment and information stored in SMTAFE information systems, are considered SMTAFE’s property and as such may accessed, moved, read, etc. as needed to meet SMTAFE business requirements.

        Statistical information derived from business information systems may be disclosed to parties outside the business only if the individuals can not be identified by the information released.

### Legal Disclaimers

Legal disclaimer shall be placed on all network access points.  Disclaimers shall be set up as a logon banner upon network logon and as a link at the bottom of all SMTAFE web pages.

### Logon Banner:

“By using this computer, you implicitly agree to the terms of the SMTAFE Information Technology Acceptable Use Policy “

### Web Disclaimer

“Information may be posted and maintained on Individual sites by SMTAFE personnel ("Individual Authors"). SMTAFE wishes to allow its users the greatest possible freedom to use these resources creatively and responsibly. However, technology services take steps to screen, verify, edit, monitor or censor information posted by Individual Authors when content is not aligned to SMTAFE goals and objectives. Individual Authors and third parties outside SMTAFE are solely responsible for the content and organization of information posted by them, even if such information is accessed through the SMTAFE World Wide Web site. Should any SMTAFE World Wide Web site user discover something out of date or in conflict with SMTAFE’s security policy or Federal or State law, please feel contact the Assistant Superintendent for Technology and Personnel.

## Network Usage Policy

        Any program adversely affecting SMTAFE information systems may be removed at the discretion of the SMTAFE Security Engineer.  Programs may be considered to adversely affect SMTAFE information systems by consuming excessive processor time, disk space, processor memory, or network bandwidth.

        Personal use of the SMTAFE network must not interfere with normal business activities.  It must not involve solicitations or be associated with any for-profit outside business activity.

* Refer to District “Staff Acceptable Use Policy.”

## Ensuring System Integrity

### Virus Protection

        It is the responsibility of each individual to scan their documents for viruses before sharing them with other people, both inside and outside of SMTAFE.

        A virus protection system shall be set up to automatically update signatures weekly.

        It is the responsibility of each individual to immediately notify the SMTAFE help desk upon finding a virus.

        All firewalls used at SMTAFE shall filter out incoming ActiveX and Java control viruses at firewall.

        The virus protection system implemented at SMTAFE shall scan attached files while in the email inbox.

        The virus protection system shall scan files immediately upon their being saving to a file server or workstation.

### Redundancy and Backups\*\*

        All business data shall be stored in at least two separate locations.

        Where possible, the SMTAFE network shall be set up to limit the number of single points of failure in the system.

        Monthly full backups shall be stored for a minimum of three months.

        As server disk become full with archived data, migration of the archived data to a Network Attached Storage (NAS) shall occur.  Two copies of the archival disk shall be made.  One copy shall be given to information owner and one copy shall be kept in safe under IT staff control.

*\*\* See Disaster Recovery Plan for more detail.*

# Security Verification

## Security Logs

All actions relative to system security must be accountable. Therefore, SMTAFE information systems shall meet the following requirements:

        System security logs shall list logon times and all other relevant security events in order to support security audits.

        System security logging shall be balanced to insure logging of relevant security information while limiting the growth of the security log to a manageable size.

         All event logs must be stored for a minimum of 2 weeks.

        A method of automatic clock synchronization shall be set up on the SMTAFE network in order to insure accurate time information in the security logs.

        All security related logs shall be reviewed on a consistent basis to ensure that SMTAFE security is not being compromised.

        Administrators shall not have rights to clear or alter security logs in order to ensure that the SMTAFE Security Engineer has accurate security information in the security log

## Security Verification Team

A security team shall be set up to test the security of the network using known techniques used by people who try to gain access to networks.  This security team shall be identified in writing to the Central Office when testing of the SMTAFE network is about to take place.  No testing of network security will take place without the authorization from Management. Upon completion of the security testing, full documentation as to the methods used and the results of the test shall be delivered to Management.

# Handling Non-compliance

Information Security Incident Management:

*a. Definition*. An information security incident includes, but is not limited to, one of the following events:

* Attempts (either failed or successful) to gain unauthorized access to a system or its data
* Unwanted disruption or denial of service
* The unauthorized use of a system for the processing or storage of data
* Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent
* Unauthorized disclosure of regulated or confidential information

*b. Notification*. Information technology employees must immediately notify their supervisor or director upon discovery of a possible or actual information security incident. Employees will immediately notify the Assistant Superintendent for Technology/Personnel if their supervisor or director is unavailable.

*c. Reporting*. Responsible information technology staff will initiate timely corrective action, document the incident and record lessons learned to prevent similar incidents from occurring in the future. The Technology Services Staff retain documentation related to all information security incidents.

*d. Exceptions.* If individuals believe they have a circumstance that requires *exception* to the SMTAFE IT Security Plan, upon agreement with the SMTAFE Network Administrators they will be allowed access or a temporary override account.  The SMTAFE Network Administrators will provide ongoing monitoring of such instances.

*It is mandatory that all employees of SMTAFE report all suspected security incidents to the SMTAFE Network Administrators*.  They may do so by making a support ticket through the SMTAFE help desk or emailing the SMTAFE Network Administrators directly.  All reported security incidents must be investigated.

# Security Awareness and Training

All individuals involved in the management, operation, programming, maintenance or use of information technology must be aware of their security responsibilities and know how to fulfill them.  To this end SMTAFE has set up the SMTAFE Security Awareness and Training program.  All individuals involved with information technology at SMTAFE shall receive an information technology security awareness briefing or be provided with appropriate information.  In addition, employees will be provided with refresher awareness material or briefings as needed.

Individuals assigned responsibilities for information technology security shall be provided with in-depth training regarding security techniques, methodologies for evaluating threats and vulnerabilities that affect specific information technology systems and applications and selection and implementation of controls and safeguards.

The SMTAFE Network Administrators shall be responsible for documenting and maintaining security training records.

# Appendix A. Local Windows Client for Netware Configuration Utility Settings

Use the following procedure to ensure security of Windows workstations.

Local Security at each workstation:

* Restrict the “Run” section of the registry. This prohibits the intrusion of spyware, malware, and other malicious programs that require utilization of this resource to operate.
* Restrictions are in place for the following workstation components: My computer, network places, control panel, screen savers, background settings, and desktop.

# Appendix B. Standard Windows 10™ Security Settings

### 

* Standard Group membership
* Rights to files and directories
* Rights to printers
* Rights to the registry
* Account Policies
* Rights listed by User and Group
* Trust relationships
* Audit Settings for Accounts, Files, Printers, and the Registry
* Event log settings

# 

# Appendix C. Firewall Policy

SMTAFE is protected by a pfSense firewall. This device allows SMTAFE the access and protection it needs while utilizing services such as authentication, wireless captive portal and VPN access. The firewall also blocks and logs intruder attempts to gain access to the SMTAFE network with the use of Snort: Intrusion Detection System (IDS).

More specific information is listed below or go to <http://www.pfsense.org/>

Getting Started

pfSense® software includes the same features as most expensive commercial firewall solutions. In some cases, pfSense includes additional features that are not available in commercial closed source solutions. In all cases, pfSense provides better value for your money. Let us show you what pfSense can do, and get you started on the path to deploying pfSense software in your environment.

Overview

The pfSense project is a free network firewall distribution, based on the FreeBSD operating system with a custom kernel and including third party free software packages for additional functionality. pfSense software, with the help of the package system, is able to provide the same functionality or more of common commercial firewalls, without any of the artificial limitations. It has successfully replaced every big-name commercial firewall you can imagine in numerous installations around the world, including Check Point, Cisco PIX, Cisco ASA, Juniper, Sonicwall, Netgear, Watchguard, Astaro, and more.

pfSense software includes a web interface for the configuration of all included components. There is no need for any UNIX knowledge, no need to use the command line for anything, and no need to ever manually edit any rule sets. Users familiar with commercial firewalls catch on to the web interface quickly, though there can be a learning curve for users not familiar with commercial-grade firewalls.

For more info: <https://www.pfsense.org/getting-started/>

# Appendix D. List of Staff who have access to the IT Infrastructure Documentation.

Kirk, James T. CEO and Senior Manager

Quinto, Spock Network Infrastructure Engineer

Jane, Trinity Network Administrator

Foster, Gloria Network Administrator