Information Security Policy

SC eLearning, LLC dba Trivantis

400 Fairway Drive, Suite 101
Deerfield Beach, FL 33441

REVISED 9.25.2019

INTRODUCTION

SCOPE

This document details the procedures and policies implemented within the Development group of SC eLearning, LLC ("Trivantis") in relation to both Trivantis and its customers. Adherence to security policies and guidelines applies to ALL development staff including: designers, developers, quality assurance testers, and support personnel.

SECURITY POLICIES – OVERVIEW

INTRODUCTION

A. Effective security is a team effort involving the participation and support of every Trivantis employee who deals with information pertaining to our customers. It is the responsibility of every employee to understand and abide by these policies. These policies extend outside of normal working hours and beyond Trivantis owned or controlled premises, and continue in full force and effect subsequent to employment termination.
B. The information that is stored by Trivantis is not extremely valuable yet may be a target of hackers, criminals, and other miscreants. Trivantis shall make every reasonable effort to safeguard such data from being compromised. This policy document describes the importance and role of the employee in the security framework of Trivantis.
C. As an employee of Trivantis, it is of primary importance to protect the integrity, and confidentiality of critical information. This information can include but is not limited to:
    1. Sensitive, proprietary company information such as trade secrets and intellectual property

2. Sensitive cardholder data including account numbers, names and addresses
    a. Note: Trivantis does not maintain credit card holder data or account numbers within its software.
3. Personally identifiable information such as social security numbers
    a. Note: Trivantis does not maintain SSN data within its software.
4. Electronic protected health information
    a. Note: Trivantis does not maintain HIPPA or other personal health data within its software. The compromise of such information could cause significant damage to the fiscal viability of Trivantis and permanently damage the reputation of the company and its employees. It is important to understand that if critical information is compromised either intentionally or unintentionally through neglect, it could result in disciplinary action including termination, as well as personal responsibilities for damages caused. It is therefore critical that each employee ensure that they are cognizant of the importance of client data and is diligent in the protection of Trivantis' customer information assets.

D. Any unauthorized copying, modifying, or destruction of client data is strictly prohibited. 1.2 PURPOSE To establish fundamental security guidelines, requirements and procedures that reduce risk and provide for the confidentiality, integrity, availability and privacy of Trivantis' information technologies and assets. The protection of information assets is mandatory for business, contractual, regulatory and legal reasons.

RESPONSIBILITIES

A. While responsibility for information systems security on a day-to-day basis is every employees duty, specific guidance, direction, and authority for information systems security is centralized for all of Trivantis employees with the Development Department. This department will perform information systems risk assessments, prepare information systems security action plans, evaluate information security products, and perform other activities necessary to assure a secure information systems environment.
B. The Development Department with cooperation with other departments will be responsible for conducting investigations into any alleged computer or network security compromises,

incidents, or issues. All significant compromises, or those posing the potential to be significant compromises, shall be immediately reported to the Chief Financial Officer (CFO).

C. System administrators, specifically the Support Team, Networking Managers, Application developers, and server administration managers are responsible for acting as local information systems security coordinators. These individuals are responsible for establishing appropriate user privileges, monitoring access control logs, and performing similar security actions for the systems they administer. System administrators also are responsible for reporting all suspicious computer and network-security-related activities to the CSO. System administrators are also responsible for implementing the requirements of this policy and other information systems security policies, standards, guidelines, and procedures.
D. All employees are responsible for complying with this and all other Trivantis policies defining computer and network security measures. All employees are also responsible for bringing all known information security vulnerabilities and violations that they notice to the attention of the CFO.

PROPRIETARY AND CONFIDENTIAL INFORMATION

A. Due to the nature of Trivantis' business operations, there is limited potential for having proprietary information stored on or in Trivantis computers and processing resources. All information stored on or in Trivantis' processing and administrative systems is considered proprietary and confidential and is not to be released to any external entity without permission from appropriate Executive personnel.
B. Upon hiring, all employees shall read and sign, thereby indicating understanding, the Agreement Concerning Confidentiality and Non-disclosure. This agreement as issued by the Chief Financial Officer (CFO) identifies the proper control, ownership and repercussions for misuse of all proprietary and confidential information.

SECURITY INVESTIGATIONS

A. If during the course of regular duties, a Trivantis employee discovers evidence of a violation of this policy, said employee shall notify the Chief Financial Officer (CFO) and the VP of Learning Information Systems. If the CFO or VP LMS determines there is probable cause to

believe a violation has occurred an additional investigation shall be authorized. The CFO or other designate of the CFO will perform any additional investigation.

B. If a member of the Support Team is requested to participate in an investigation of improper use committed by a client, or if Trivantis personnel notices evidence of improper use upon viewing a client's files (after receiving consent) during the normal course of job duties, that member of the Support Team shall be careful not to disclose information about that client or the contents of the client's files to others.
C. Information concerning the client shall only be disclosed to the CFO or VP LMS, or to a law enforcement agency as necessary. It is extremely important to keep a detailed record of all actions when investigating an allegation of improper use.

EMPLOYEE BACKGROUND VERIFICATION

A. All potential Trivantis employees undergo a pre-employment background check investigating criminal records, credit history and reference checks. A personal background by an external third party delivering a document to the CFO.
B. The CFO collects relevant personal information from all new and potential employees and maintains a record of the information. If any issues are uncovered during the hiring process the prospect is informed they will not meet the Trivantis security policy.

SECURITY POLICY REVIEW

Trivantis' security policies will be reviewed annually. Any changes to this policy will be approved by Trivantis CFO and Legal counsel before distribution. If a Trivantis employee wishes to make a policy recommendation, the request must be submitted to the CFO with the following information.

A. Describe the new or updated policy
B. Provide a reason or justification for new or updated policy and identify the risks of not implementing changes
C. List the major impacts of implementation, compliance, and enforcement (business or technical)
D. Identify the impacted stakeholders

E. Identify the dependencies for implementation of policy changes (i.e. project, regulatory, technology, or organization)

MANAGEMENT COMMITMENT

Trivantis management is committed to ensuring the policies outlined in this document are followed, enforced, and ultimately embraced. Security is more than just a series of checkboxes and procedures, rather it is a culture. Management strives to cultivate this culture throughout all facets of Trivantis to help reduce risk and ensure the confidentiality, integrity, and availability of corporate assets.

SECURITY AWARENESS AND TRAINING

GENERAL SECURITY AWARENESS

All managers must continually strive to incorporate information security into training courses, internal newsletters, posters, and other tools and visual aids to increase information security awareness among all personnel.

ANNUAL TRAINING

All personnel must participate at least annually in ongoing information security awareness and training activities as required.

INFORMATION RESOURCE OPERATIONAL SECURITY TRAINING

For confidential and critical information resources, appropriate operational security training must be developed and conducted. For business-controlled information resources, it is recommended that appropriate operational security training be developed and conducted.

NEW PERSONNEL TRAINING

All new personnel must receive information security training. The CFO in coordination with the employees manager will review the security policy and non-disclosure agreement along with the security training course.

WORKSTATION SECURITY POLICY

INTRODUCTION

Trivantis Development and Support personnel workstations that are all behind firewalls so that no individual machine is ever directly connected to the external internet. This ensures that no development machine is ever the target of an external entity that is trying to breach our systems to gain access to sensitive corporate or customer data.

PURPOSE

The purpose of this policy is define how Trivantis controls and implements workstation security to ensure confidentiality, integrity and availability of information contained on Trivantis and client solutions.

POLICY

A. All employees are required to connect to the Trivantis network via local area networks that are firewalled. In addition, no port forwarding will be enabled on any of the externally facing devices to prevent unauthorized access to Trivantis resources.
B. All employees must lock their respective sessions when away for any reason or any duration of time, no matter how minimal.

PHYSICAL SECURITY POLICY

INTRODUCTION

Trivantis will protect its information resources through implementation of sound physical, environmental, and administrative security controls designed to reduce the risk of physical failure of infrastructure components, damage from natural or fabricated environmental hazards, and use by unauthorized personnel.

POLICY

A. It is Trivantis' policy that individual employee badge access will be audited annually. Badges will be valid for one year. If the individual has additional access beyond their departmental role access (Special Access), it must be re-authorized by an authorized party as defined in the security procedures.
B. Clients and contractors will not be issued badge access.

C. All Trivantis operated access control systems shall be monitored by for authentication success, failures, and alarms 24/7/365. Additionally, Trivantis Office access is monitored via video surveillance systems. The video coverage and retention times may vary between facilities.
D. If a breach is discovered or suspected, the employee shall immediately report the incident through the appropriate chain of management. Any and all suspicious activity must be immediately reported.
E. Access to the Trivantis Development Center is highly restricted. Specifically, all physical access smartcards shall be authorized and will only be granted to areas required for job functions. If you see employees or other individuals in a restricted area of the facility without a proper escort or badge report it immediately.
F. All visitors and contractors must sign-in to the appropriate log book. The log will contain at minimum, the visitor's name, their company, and the employee authorizing physical access.

KEYS AND KEYCARDS

It is important that security is maintained in all Trivantis facilities at all times. If you are provided with a key, verify that the key is with you at all times and that nobody else has access to it. The key is for your individual only. If you lose your key, report this to your supervisor immediately.

NO PIGGYBACKING

Trivantis' policy states that unauthorized personnel must not be allowed access to Trivantis' facilities. When entering or exiting a secure doorway, verify that the door is closed behind you. Do not hold the door open for other parties or leave the door propped open.

MEDIA CONTROL POLICY

INTRODUCTION

This policy details the control methods for media required to maintain the highest possible level of information security.

PURPOSE

A. This policy shall define and classify critical systems and data, and specify which departments may access said systems and data as a part of their job function.

B. This document applies to all electronically stored media, hardcopy media, critical systems and confidential data not necessarily attached to a particular medium.

POLICY

All data will be automatically backed up daily from an employee’s workstation to the central development server at the Development Center. That server will then be nightly backed up via secure transfer to the Trivantis corporate data repository.

No backups via CD Rom, external removable media, or transfer via FTP will be allowed for any source materials or data.

Customer data will never be loaded onto Trivantis servers without the express permission from the customer in question. This should only be used in scenarios under which the customer data is the only way to illustrate a particular problem. If customer data is loaded to a Trivantis employee’s machine, that data and all copies of it will be deleted at the conclusion of the project that necessitated access to the data.

A. Trivantis resources and customer data will never be allowed to be loaded to non-Trivantis owned hardware.
B. Personal computers and removable media will not be allowed to be connected to Trivantis development networks.

NETWORK USAGE POLICY

INTRODUCTION

This policy details local access connections to the Trivantis network.

PURPOSE

The purpose of this policy is to define the restrictions to connecting to Trivantis' wired and wireless networks.

POLICY

The following network activities are prohibited on Trivantis' LAN or WLAN.

A. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
B. Port scanning or security scanning is expressly prohibited unless required or requested as part of a Trivantis hosting solution.
C. Executing any form of network monitoring which will intercept data not intended for the employee or client unless this activity is a part of the employee's normal job/duty.
D. It is prohibited to setup rogue access points or to utilize wireless ad-hoc networks.

LAN (WIRED) NETWORK USAGE

It is prohibited to connect any unauthorized network device to any Trivantis Ethernet port including but not limited to the Data Center, Office, and lab environments.

WLAN (WIRELESS) NETWORK USAGE

Trivantis employees are allowed to use their wireless devices to connect to the Trivantis WLAN. 'Trivantis' is a WPA2 restricted wireless access point requiring token authentication and is completely segregated from all development Trivantis network resources. In order to access internal resources, employees must VPN, requiring an additional token authentication.

PROHIBITED ACTIVITY POLICY

INTRODUCTION

A. The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).
B. Under no circumstances is an employee of Trivantis authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Trivantis-owned resources.

C. Trivantis IT systems and accounts are to be used only for the purpose for which they are authorized and are not to be used for non-Trivantis related activities. Unauthorized use of a Trivantis account and/or system is a violation of Section 799, Title 18, U.S. Code, constitutes theft, and is punishable by law. Therefore, unauthorized use of Trivantis IT computing systems and facilities may constitute grounds for dismissal and either civil or criminal prosecution.

PURPOSE

The purpose of the policies below is by no means exhaustive, but attempts to provide a framework for activities which fall into the category of unacceptable use.

POLICY

A. Unacceptable Activity Use includes the following:
    1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Trivantis.
    2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Trivantis or the end user does not have an active license is strictly prohibited.
    3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
    4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).
    5. Revealing your account password to others or allowing use of your account by others.

6. Using a Trivantis computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any Trivantis account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Circumventing user authentication or security of any host, network or account.
10. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
11. Providing any information about Trivantis employees to parties outside of the Trivantis Community.
12. Users shall not make copies of system configuration files for their own, unauthorized personal use or to provide to others.

B. Users shall not download, install or run security programs or utilities that reveal weaknesses in the security of any system. For example, Users shall not run password-cracking programs, "network sniffer" utilities or other sleuthing or tracing programs on Trivantis IT computing systems.

EMAIL USE POLICY

INTRODUCTION

The Trivantis email systems are used to allow effective communication between employees, clients, and business associates. Email transmission over the internet is inherently insecure and subject to security breaches that include message interception, message alteration, and spoofing. Users of the Trivantis email systems should not assume the confidentiality or integrity of any message that is sent or received via the Internet.

PURPOSE

The purpose of this policy is to define appropriate and inappropriate use of the Trivantis email system.

POLICY

PROHIBITED USE

The Trivantis email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin, as well as confidential information such as cardholder information, IP addresses, credentials, customer account information, network diagrams, and encryption and decryption keys. Employees who receive any emails with this content from any Trivantis employee should report the matter to their supervisor immediately.

PERSONAL USE

Using a reasonable amount of Trivantis resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work-related email.

MONITORING

Trivantis employees shall have no expectation of privacy in anything they store, send or receive on the company's email system. Trivantis may monitor messages without prior notice. Trivantis is not obliged to monitor email messages.

ENCRYPTION POLICY

INTRODUCTION

Encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

PURPOSE

The purpose of this policy is to enforce a standard that limits the use of encryption techniques to only Trivantis approved algorithms and utilities which will securely transmit sensitive data to ensure confidentiality and integrity of confidential information over the internet.

POLICY

A. Trivantis deploys strong cryptography based on industry-tested and accepted algorithms, along with strong key lengths and proper key-management practices. Cryptography includes both encryption (which is reversible) and hashing (which is not reversible, or “one way”). SHA-1 is an example of an industry-tested and accepted hashing algorithm. Examples of industry-tested and accepted standards and algorithms for encryption include AES (128 bits and higher), TDES (minimum double-length keys), RSA (1024 bits and higher), ECC (160 bits and higher), and ElGamal (1024 bits and higher).
B. Whenever password information is to be stored in a database, it must be encrypted in accordance with this policy for storage.
C. When userids/passwords are transmitted between the workstation and a Trivantis online system, those items must be encrypted as to prevent their being captured as plaintext.
D. When exporting software/data to foreign companies, all efforts must be made to keep in compliance with the Bureau of Export Administration (BXA) (http://www.bxa.doc.gov/) restrictions on cryptographic export.

INSTANT MESSAGING POLICY

INTRODUCTION

The use of Instant Messaging and IRC systems, also known as Chat is a form of real-time communication between two or more people based on typed text. Instant messaging and IRC are a critical part of Trivantis internal communication system. It is important to understand the acceptable use of this technology in the Trivantis environment.

PURPOSE

Instant Messaging and IRC is limited to the capabilities provided by Trivantis on internal network systems. All employees must use the Instant Messaging and IRC service provided in a manner that protects company assets and confidential Information.

POLICY

A. Trivantis leverages Connections (IBM) and IRC as an internal communication medium. These messaging protocols send data encrypted between two or more parties. Employees should be logged into Connections throughout their workday and optionally IRC. This will allow other employees to know you are in the office and they can communicate with you instantly. Since Connections and IRC use SSL, sending certain types of confidential data through these systems is permitted. Connections also has an option for multi-user conference. You are encouraged to use these conferences to communicate with employees in you department.
B. Sending confidential information via any other instant messaging server is strictly prohibited.

REMOTE ACCESS POLICY

INTRODUCTION

Remote access allows employees to connect to Trivantis application servers so they may continue to work when outside the Trivantis facilities.

PURPOSE

The purpose of this policy is to define standards for connecting to Trivantis' network from any host outside the Trivantis network (e.g. mobile or employee owned computers). These standards are designed to minimize the potential exposure to Trivantis from damages which may result from unauthorized use of Trivantis' resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Trivantis internal systems, etc.

POLICY

A. Only manager approved employees will be allowed to remotely connect to Trivantis application servers to work from outside the Trivantis facilities. No external computers (e.g. mobile devices or employee owned computers) can connect directly to client solutions. Once an employee is authenticated via VPN, employees will be restricted to their application servers to which they normally have access.

B. Employees who require remote access must get permission from their development manager to access the Trivantis Development VPN.

PASSWORD POLICY

INTRODUCTION

A. In computing, a password is a word or string of characters, entered, often along with a user name, into a computer system to log in or to gain access to some resource. Passwords are a popular form of authentication. Full security requires that the password be kept.
B. The length, complexity, and secrecy of a password are vital to prevent compromise.

PURPOSE

The purpose of this policy is to identify the characteristics of strong passwords and use them accordingly.

POLICY

A. It is the policy of Trivantis that everyone be aware of how to select strong passwords. Poor, weak passwords have the following characteristics:
    1. The password contains less than eight characters
    2. The password is a word found in a dictionary (English or foreign)
    3. The password is a common usage word such as:
        a. Names of family, pets, friends, co-workers, fantasy characters, etc.
        b. Computer terms and names, commands, hardware, software.
        c. The company name (Trivantis), city, street or any other unique company indicator.
        d. Birthdays and other personal information such as addresses and phone numbers.
        e. Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
        f. Any of the above spelled backwards.
        g. Any of the above preceded or followed by a digit (e.g., secret1, 1secret)
B. Strong passwords have the following characteristics:

1. Contain both upper and lower case characters (e.g., a-z, A-Z)
2. Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=`{}[]:";'<>?,./)
3. Are at least eight alphanumeric characters in length.
4. Are not words in any language, slang, dialect, jargon, etc.
5. Are not based on personal information, names of family, etc.

C. Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation. NOTE: Do not use either of these examples as passwords!

PASSWORD PROTECTION STANDARDS

A. Do not use the same password for Trivantis accounts as for other non-Trivantis access (e.g., personal ISP account, option trading, benefits, etc.).

B. Where possible, don't use the same password for various Trivantis access needs. For example, select one password for the special access (administrative) and a separate password for screensaver. A

C. Do not share Trivantis passwords with anyone. All passwords are to be treated as Sensitive Trivantis information.

D. Additional Password "Don'ts:"
1. Don't reveal a password over the phone to ANYONE
2. Don't reveal a password in an email message
3. Don't reveal a password to your team manager
4. Don't talk about a password in front of others
5. Don't hint at the format of a password (e.g., "my family name")
6. Don't reveal a password on questionnaires or security forms
7. Don't share a password with family members
8. Don't reveal a password to co-workers while on vacation

E. If someone demands a password, refer them to this document or have them call someone in the Security Department.

F. Do not use the "Remember Password" feature of applications (e.g., Internet Explorer and Firefox)
G. Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.
H. If an account or password is suspected to have been compromised, report the incident the CSO and change all passwords.
I. Password cracking or guessing may be performed on a periodic or random basis by the CSO or his/her delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.
J. Recommended password encryption storage programs are KeePass and Password Agent.

PIN SELECTION STANDARDS

A. Numbers should always be used when available.
B. Avoid ascending and descending number sequences
C. Avoid common dates such as birthdays and other personal information.

USER ACCOUNT MANAGEMENT

INTRODUCTION

Computer accounts are the means used to grant access to Trivantis' Information Resources. These accounts provide a means of providing accountability, a key to any computer security program, for Information Resources usage. This means that creating, controlling, and monitoring all computer accounts is extremely important to an overall security program.

PURPOSE

The purpose of this policy is to establish the rules for the creation, monitoring, control and removal of user accounts.

POLICY

A. All accounts created must have an associated request and approval that is appropriate for the Trivantis system or service.
B. First time account passwords must be a random password with "reset password on next logon" checked.
C. All accounts must be uniquely identifiable using the assigned user name.
D. All default passwords for accounts must be constructed in accordance with the Trivantis Password Policy.
E. All accounts must require passwords to be changed every 90 days.
F. Accounts of individuals on extended leave (more than 30 days) will be disabled.
G. All new user accounts that have not been accessed within 30 days of creation will be disabled.
H. IT or other designated staff:
    1. Are responsible for removing the accounts of individuals who change roles within Trivantis, or are separated from their relationship with Trivantis.
    2. Must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes.
    3. Must have a documented process for periodically reviewing existing accounts for validity.
    4. Are subject to independent audit review.
    5. Must provide a list of accounts for the systems they administer when requested by authorized Trivantis management.
    6. must cooperate with authorized Trivantis management investigating security incidents

ACCESS BY LEAST PRIVILEGE

Access privileges are granted to Trivantis employees based on departmental role. Roles have been granted the least privilege necessary to perform their job function. IT assigns the roles at the time of employment or positions reassignment.

MOBILE DEVICE PROTECTION POLICY

INTRODUCTION

Implementing mobile device protection greatly reduces the risk of sensitive data being exposed if an unauthorized person had the mobile device in their possession.

PURPOSE

The purpose of this policy is to describe the Information Security requirements for protecting data at rest on Trivantis mobile devices.

POLICY

A. All mobile devices containing stored data owned by Trivantis must use an approved method of encryption to protect data at rest. Mobile devices are defined to include laptops, PDAs, and smart phones.
B. Users are expressly forbidden from storing Trivantis data on devices that are not issued by Trivantis, such as storing Trivantis email on a personal smart phone or PDA.
C. Users are expressly forbidden from storing any client data on any Trivantis mobile device. It also prohibited utilizing any software which relays Trivantis credentials to a third party. For example, instant messengers on smart phones which proxy connections.
D. Personal firewalls on mobile devices are not required on employee mobile devices. Trivantis's network architecture prevents direct connections to the network by enforcing a two factor authentication VPN to a jump host before an employee will be able to reach any Trivantis resource.

PDAS AND SMART PHONES

Any PDA or smart phones that contain Trivantis information must have a security policy to auto lock after inactivity and wipe the device after 10 unsuccessfully password attempts. The password or PIN used to lock the mobile device must also adhere to Trivantis' password policy.

LOSS AND THEFT

The loss or theft of any mobile device containing Trivantis data must be reported immediately.

EMPLOYEE TERMINATION

INTRODUCTION

It is necessary for prompt and complete revocation of a terminated employee's access and company owned assets to address the associated risk of interacting with company resources post termination.

PURPOSE

To ensure proper termination procedures are performed in a timely manner.

POLICY

In the event of a terminated employee, department managers must be notified, access to any Trivantis resource must be immediately revoked, and all company-owned property must be dispossessed. The Trivantis Human resources department is responsible for collecting all company-owned property such as mobile devices, tokens, keys, access cards, and notifying department managers before the terminated employee is escorted out of the Trivantis facility. Immediately after receiving a terminated employee notification, responsible parties shall revoke all facility, computer, network, and data access from said employee.

SPECIAL ACCESS AGREEMENT

OVERVIEW

A. As a Trivantis employee, your current or future role may call for you to administer client resources. These resources may require 'root', 'administrator', or 'enable' level access in order for you to perform your job ("Special Access"). Special Access levels grant the operator unrestricted access to view, modify, or delete system settings and data. This data may contain confidential information including, but not limited to credit card data, trade secrets, or encryption keys ("Confidential Data"). You are responsible for all actions performed on any client resource. It is prohibited and shall be cause for termination to maliciously modify or delete any system settings or data, or to disclose or transmit any such Confidential Data in an unencrypted form.

B. In addition to the aforementioned requirements, the following Special Access Guidelines have been developed to help people use Special Access rights in a responsible and secure manner.

GENERAL GUIDELINES

BE AWARE OF THE TRIVANTIS ENVIRONMENT

Each Trivantis facility is highly specialized and contains numerous computing systems and equipment of differing configurations and functions. The proper use of these resources is documented in the appendices of Trivantis' Organizational Security Policy. It is the responsibility of all employees to READ, UNDERSTAND and ADHERE to the procedures and policies detailed within the Organizational Security Policy.

USE SPECIAL ACCESS ONLY IF NECESSARY

Many system tasks require the use of root or other special access. However, there are many tasks that can be performed without the use of Special Access. When possible, use regular accounts for troubleshooting and investigating.

DOCUMENT ALL MAJOR ACTIONS AND/OR INFORM APPROPRIATE PERSONNEL

Documentation provides a method to analyze events. In the future, others may want to know what was performed to address a certain problem. The applicable Team Manager is to be informed BEFORE any changes are made to system-specific or configuration files.

HAVE A BACKUP PLAN IN THE EVENT SOMETHING GOES WRONG

Special Access, especially root, has a tremendous potential for causing damage with only a few keystrokes. Develop a backup plan in the event something goes wrong. You must be able to restore the system to its prior approved state.

KNOW WHOM TO TURN TO IF PROBLEMS ARISE

Through the use of Special Access, new and unique problems and/or situations may arise. Although Trivantis has many written procedures, they do not cover every possible scenario. If any doubt exists as to how you should trouble-shoot a problem, ask for assistance. Know whom to ask.

SPECIFIC RESTRICTIONS

A. Do not share Special Access passwords with anyone.
B. Do not write down Special Access passwords or the current algorithm.
C. Do not routinely log onto a system, for which you have an account, as “root” or any other Special Access account unless it is absolutely necessary.
D. Do not read or send personal mail, play games, read the net news or edit personal files using a Special Access account.
E. Do not browse other user’s files, directories or email using a Special Access account unless the proper permission has been granted.
F. Do not make a change on any system that is not directly related to your job duties
G. Do not use Special Access to create temporary files or directories for your own personal use.