Corporate Security Policies

Corporate Security

- Acceptable Use Policy
- Backup Policy
- Confidential Data Policy
- Consumer Disputes Policy
- Criminal Database Searches Policy
- Data Classification Policy
- Encryption Policy
- Guest Access Policy
- Incident Response Policy
- Mobile Device Policy
- Network Access & Authentication policy
- Network Security Policy
- Outsourcing Policy
- Password Policy
- Physical Security Policy
- Remote Access Policy
- Retention Policy
- Third Party Connection Policy
- VPN Policy
- Wireless Access Policy

TruDiligence, LLC

Acceptable Use Policy	Created: 3/3/2009
Section of: Corporate Security Policies	Target Audience: Users, Technical
CONFIDENTIAL	Page 1 of 8

TruDiligence, LLC is hereinafter referred to as "the company."

1.0 Overview

Though there are a number of reasons to provide a user network access, by far the most common is granting access to employees for performance of their job functions. This access carries certain responsibilities and obligations as to what constitutes acceptable use of the corporate network. This policy explains how corporate information technology resources are to be used and specifies what actions are prohibited. While this policy is as complete as possible, no policy can cover every situation, and thus the user is asked additionally to use common sense when using company resources. Questions on what constitutes acceptable use should be directed to the user's supervisor.

2.0 Purpose

Since inappropriate use of corporate systems exposes the company to risk, it is important to specify exactly what is permitted and what is prohibited. The purpose of this policy is to detail the acceptable use of corporate information technology resources for the protection of all parties involved.

3.0 Scope

The scope of this policy includes any and all use of corporate IT resources, including but not limited to, computer systems, email, the network, and the corporate Internet connection.

4.0 Policy

4.1 E-mail Use

Personal usage of company email systems is permitted as long as A) such usage does not negatively impact the corporate computer network, and B) such usage does not negatively impact the user's job performance.

- The following is never permitted: spamming, harassment, communicating threats, solicitations, chain letters, or pyramid schemes. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are prohibited.

- The user is prohibited from forging email header information or attempting to impersonate another person.

- Email is an insecure method of communication, and thus information that is considered confidential or proprietary to the company may not be sent via email, regardless of the recipient, without proper encryption.

- It is company policy not to open email attachments from unknown senders, or when such attachments are unexpected.

- Email systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size.

4.2 Confidentiality

Confidential data must not be A) shared or disclosed in any manner to non-employees of the company, B) should not be posted on the Internet or any publicly accessible systems, and C) should not be transferred in any insecure manner. Please note that this is only a brief overview of how to handle confidential information, and that other policies may refer to the proper use of this information in more detail.

4.3 Network Access

The user should take reasonable efforts to avoid accessing network data, files, and information that are not directly related to his or her job function. Existence of access capabilities does not imply permission to use this access.

4.4 Unacceptable Use

The following actions shall constitute unacceptable use of the corporate network. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are deemed unacceptable. The user may not use the corporate network and/or systems to:

- Engage in activity that is illegal under local, state, federal, or international law.

- Engage in any activities that may cause embarrassment, loss of reputation, or other harm to the company.

- Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media.

- Engage in activities that cause an invasion of privacy.

- Engage in activities that cause disruption to the workplace environment or create a hostile workplace.

- Make fraudulent offers for products or services.

- Perform any of the following: port scanning, security scanning, network sniffing, keystroke logging, or other IT information gathering techniques when not part of employee's job function.

- Install or distribute unlicensed or "pirated" software.

- Reveal personal or network passwords to others, including family, friends, or other members of the household when working from home or remote locations.

4.5 Blogging

Blogging by the company's employees is subject to the terms of this policy, whether performed from the corporate network or from personal systems. Blogging is never allowed from the corporate computer network. In no blog, including blogs published from personal or public systems, shall the company be identified, company business matters discussed, or material detrimental to the company published. The user must not identify himself or herself as an employee of the company in a blog. The user assumes all risks associated with blogging.

4.6 Instant Messaging

Instant Messaging is allowed for corporate communications only. The user should recognize that Instant Messaging may be an insecure medium and should take any necessary steps to follow guidelines on disclosure of confidential data.

4.7 Overuse

Actions detrimental to the computer network or other corporate resources, or that negatively affect job performance are not permitted.

4.8 Web Browsing

The Internet is a network of interconnected computers of which the company has very little control. The user should recognize this when using the Internet, and understand that it is a public domain and he or she can come into contact with information, even inadvertently, that he

or she may find offensive, sexually explicit, or inappropriate. The user must use the Internet at his or her own risk. The company is specifically not responsible for any information that the user views, reads, or downloads from the Internet.

Personal Use. The company recognizes that the Internet can be a tool that is useful for both personal and professional purposes. Personal usage of company computer systems to access the Internet is permitted as long as long as such usage follows pertinent guidelines elsewhere in this document and does not have a detrimental effect on the company or on the user's job performance.

4.9 Copyright Infringement

The company's computer systems and networks must not be used to download, upload, or otherwise handle illegal and/or unauthorized copyrighted content. Any of the following activities constitute violations of acceptable use policy, if done without permission of the copyright owner: A) copying and sharing images, music, movies, or other copyrighted material using P2P file sharing or unlicensed CD's and DVD's; B) posting or plagiarizing copyrighted material; and C) downloading copyrighted files which employee has not already legally procured. This list is not meant to be exhaustive, copyright law applies to a wide variety of works and applies to much more than is listed above.

4.10 Peer-to-Peer File Sharing

Peer-to-Peer (P2P) networking is not allowed on the corporate network under any circumstance.

4.11 Streaming Media

Streaming media can use a great deal of network resources and thus must be used carefully. Reasonable use of streaming media is permitted as long as it does not negatively impact the computer network or the user's job performance.

4.12 Monitoring and Privacy

Users should expect no privacy when using the corporate network or company resources. Such use may include but is not limited to: transmission and storage of files, data, and messages. The company reserves the right to monitor any and all use of the computer network. To ensure compliance with company policies this may include the interception and review of any emails, or other messages sent or received, inspection of data stored on personal file directories, hard disks, and removable media.

4.13 Bandwidth Usage

Excessive use of company bandwidth or other computer resources is not permitted. Large file downloads or other bandwidth-intensive tasks that may degrade network capacity or performance must be performed during times of low company-wide usage.

4.14 Personal Usage

Personal usage of company computer systems is permitted as long as long as such usage follows pertinent guidelines elsewhere in this document and does not have a detrimental effect on the company or on the user's job performance.

4.15 Remote Desktop Access

Use of remote desktop software and/or services is allowable as long as it is provided by the company. Remote access to the network must conform to the company's Remote Access Policy.

4.16 Circumvention of Security

Using company-owned or company-provided computer systems to circumvent any security systems, authentication systems, user-based systems, or escalating privileges is expressly prohibited. Knowingly taking any actions to bypass or circumvent security is expressly prohibited.

4.17 Use for Illegal Activities

No company-owned or company-provided computer systems may be knowingly used for activities that are considered illegal under local, state, federal, or international law. Such actions may include, but are not limited to, the following:

- Unauthorized Port Scanning
- Unauthorized Network Hacking
- Unauthorized Packet Sniffing
- Unauthorized Packet Spoofing
- Unauthorized Denial of Service
- Unauthorized Wireless Hacking
- Any act that may be considered an attempt to gain unauthorized access to or escalate privileges on a computer or other electronic system

- Acts of Terrorism
- Identity Theft
- Spying
- Downloading, storing, or distributing violent, perverse, obscene, lewd, or offensive material as deemed by applicable statues
- Downloading, storing, or distributing copyrighted material

The company will take all necessary steps to report and prosecute any violations of this policy.

4.18 Non-Company-Owned Equipment

The user must obtain written permission from the IT Manager before installing outside or non-company-provided computer systems on the company network. Once this permission is obtained, and dependent on any conditions granted along with such permission, the user can connect a non-company-owned system to the network. Reasonable precautions must be taken to ensure viruses, Trojans, worms, malware, spyware, and other undesirable security risks are not introduced onto the company network.

4.19 Personal Storage Media

The company does not restrict the use personal storage media, which includes but is not limited to: USB or flash drives, external hard drives, personal music/media players, and CD/DVD writers, on the corporate network provided that guidelines for data confidentiality are followed. The user must take reasonable precautions to ensure viruses, Trojans, worms, malware, spyware, and other undesirable security risks are not introduced onto the company network. Use of personal storage media must conform to the company's Mobile Device Policy.

4.20 Software Installation

Installation of non-company-supplied programs is prohibited. Numerous security threats can masquerade as innocuous software - malware, spyware, and Trojans can all be installed inadvertently through games or other programs. Alternatively, software can cause conflicts or have a negative impact on system performance.

4.21 Reporting of Security Incident

If a security incident or breach of any security policies is discovered or suspected, the user must

immediately notify his or her supervisor and/or follow any applicable guidelines as detailed in the corporate Incident Response Policy. Examples of incidents that require notification include:

- Suspected compromise of login credentials (username, password, etc.).
- Suspected virus/malware/Trojan infection.
- Loss or theft of any device that contains company information.
- Loss or theft of ID badge or keycard.
- Any attempt by any person to obtain a user's password over the telephone or by email.
- Any other suspicious event that may impact the company's information security.

Users must treat a suspected security incident as confidential information, and report the incident only to his or her supervisor. Users must not withhold information relating to a security incident or interfere with an investigation.

4.22 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 Manager and/or executive 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 are suspected, the company will report such activities to the applicable authorities. If any provision of this policy is found to be unenforceable or voided for any reason, such invalidation will not affect any remaining provisions, which will remain in force.

6.0 Definitions

Blogging The process of writing or updating a "blog," which is an online, user-created journal (short for "web log").

Instant Messaging A text-based computer application that allows two or more Internet-connected users to "chat" in real time.

Peer-to-Peer (P2P) File Sharing A distributed network of users who share files by directly connecting to the users' computers over the Internet rather than through a central server.

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.

Streaming Media Information, typically audio and/or video, that can be heard or viewed as it is being delivered, which allows the user to start playing a clip before the entire download has completed.

7.0 Revision History

Revision 1.2 4/30/2008

TruDiligence, LLC

Backup Policy	Created: 3/3/2009
Section of: Corporate Security Policies	Target Audience: Technical
CONFIDENTIAL	Page 1 of 4

TruDiligence, LLC 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.

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) and email 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.

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.

Incremental: every day
Full: every 3 days

4.4 Off-Site Rotation

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 Company's uptime requirements. The company has determined that backup media must be rotated off-site at least once per 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.

When stored onsite, backups should be kept in an access-controlled area. When shipped off-site, a hardened facility (i.e., commercial backup service or safe deposit box) that uses accepted methods of environmental controls, including fire suppression, and security processes must be used to ensure the integrity of the backup media. 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 policy and any industry regulations, if applicable):

Incremental Backups must be saved for one week.
Full Backups must be saved for one month.

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 twice per year.

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

The backup policy will be enforced by the designated backup administrator, the IT Manager, and/or the executive team; and should be validated through periodic audit. Violations may

result in disciplinary action, which may include suspension or more severe penalties up to and including termination of employment.

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 Also called "recovery." 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.

7.0 Revision History

Revision 1.2 4/30/2008

TruDiligence, LLC

Confidential Data Policy	Created: 3/3/2009
Section of: Corporate Security Policies	Target Audience: Users, Technical
CONFIDENTIAL	Page 1 of 6

TruDiligence, LLC is hereinafter referred to as "the company."

1.0 Overview

Confidential data is typically the data that holds the most value to a company. Often, confidential data is valuable to others as well, and thus can carry greater risk than general company data. For these reasons, it is good practice to dictate security standards that relate specifically to confidential data.

2.0 Purpose

The purpose of this policy is to detail how confidential data, as identified by the Data Classification Policy, should be handled. This policy lays out standards for the use of confidential data, and outlines specific security controls to protect this data.

3.0 Scope

The scope of this policy covers all company-confidential data, regardless of location. Also covered by the policy are hardcopies of company data, such as printouts, faxes, notes, etc.

4.0 Policy

4.1 Treatment of Confidential Data

For clarity, the following sections on storage, transmission, and destruction of confidential data are restated from the Data Classification Policy.

4.1.1 Storage

Confidential information must be removed from desks, computer screens, and common areas unless it is currently in use. Confidential information should be stored under lock and key (or keycard/keypad), with the key, keycard, or code secured.

4.1.2 Transmission

Strong encryption must be used when transmitting confidential data, regardless of whether such transmission takes place inside or outside the company's network. Confidential data must not be left on voicemail systems, either inside or outside the

company's network, or otherwise recorded.

4.1.3 Destruction

Confidential data must be destroyed in a manner that makes recovery of the information impossible. The following guidelines apply:

- Paper/documents: cross cut shredding is required.
- Storage media (CD's, DVD's): physical destruction is required.
- Hard Drives/Systems/Mobile Storage Media: physical destruction is required. If physical destruction is not possible, the IT Manager must be notified.

4.2 Use of Confidential Data

A successful confidential data policy is dependent on the users knowing and adhering to the company's standards involving the treatment of confidential data. The following applies to how users must interact with confidential data:

- Users must be advised of any confidential data they have been granted access. Such data must be marked or otherwise designated "confidential."
- Users must only access confidential data to perform his/her job function.
- Users must not seek personal benefit, or assist others in seeking personal benefit, from the use of confidential information.
- Users must protect any confidential information to which they have been granted access and not reveal, release, share, email unencrypted, exhibit, display, distribute, or discuss the information unless necessary to do his or her job or the action is approved by his or her supervisor.
- Users must report any suspected misuse or unauthorized disclosure of confidential information immediately to his or her supervisor.
- If confidential information is shared with third parties, such as contractors or vendors, a confidential information or non-disclosure agreement must govern the third parties' use of confidential information. Refer to the company's outsourcing policy for additional guidance.
- If confidential information is shared with a third party, the company must indicate to the

third party how the data should be used, secured, and, destroyed. Refer to the company's outsourcing policy for additional guidance.

4.3 Security Controls for Confidential Data

Confidential data requires additional security controls in order to ensure its integrity. The company requires that the following guidelines are followed:

- Strong Encryption. Strong encryption must be used for confidential data transmitted internal or external to the company. Confidential data must always be stored in encrypted form, whether such storage occurs on a user machine, server, laptop, or any other device that allows for data storage.

- Network Segmentation. The company must use firewalls, access control lists, or other security controls to separate the confidential data from the rest of the corporate network.

- Authentication. Two-factor authentication must be used for access to confidential data.

- Physical Security. Systems that contain confidential data, as well as confidential data in hardcopy form, should be stored in secured areas. Special thought should be given to the security of the keys and access controls that secure this data.

- Printing. When printing confidential data the user should use best efforts to ensure that the information is not viewed by others. Printers that are used for confidential data must be located in secured areas.

- Faxing. When faxing confidential data, users must use cover sheets that inform the recipient that the information is confidential. Faxes should be set to print a confirmation page after a fax is sent; and the user should attach this page to the confidential data if it is to be stored. Fax machines that are regularly used for sending and/or receiving confidential data must be located in secured areas.

- Emailing. Confidential data must not be emailed inside or outside the company without the use of strong encryption.

- Mailing. If confidential information is sent outside the company, the user must use a service that requires a signature for receipt of that information. When sent inside the company, confidential data must be transported in sealed security envelopes marked "confidential."

- Discussion. When confidential information is discussed it should be done in non-public

places, and where the discussion cannot be overheard.

- Confidential data must be removed from documents unless its inclusion is absolutely necessary.

- Confidential data must never be stored on non-company-provided machines (i.e., home computers).

- If confidential data is written on a whiteboard or other physical presentation tool, the data must be erased after the meeting is concluded.

4.4 Examples of Confidential Data

The following list is not intended to be exhaustive, but should provide the company with guidelines on what type of information is typically considered confidential. Confidential data can include:

- Employee or customer social security numbers or personal information
- Medical and healthcare information
- Customer data
- Company financial data (if company is closely held)
- Sales forecasts
- Product and/or service plans, details, and schematics,
- Network diagrams and security configurations
- Communications about corporate legal matters
- Passwords
- Bank account information and routing numbers
- Payroll information
- Credit card information

- Any confidential data held for a third party (be sure to adhere to any confidential data agreement covering such information)

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 Manager and/or executive 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 will report such activities to the applicable authorities.

6.0 Definitions

Authentication A security method used to verify the identity of a user and authorize access to a system or network.

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.

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

Two-Factor Authentication A means of authenticating a user that utilizes two methods: something the user has, and something the user knows. Examples are smart cards, tokens, or biometrics, in combination with a password.

U.S. DoD Standards Stands for United States Department of Defense Standards. Standards on data destruction detailed in DoD 5220.22-M. Most data wiping software packages provide an option for wiping to this standard.

7.0 Revision History

Revision 1.2 4/30/2008

TruDiligence, LLC

Consumer Disputes	Created: 3/3/2009
Section of: Corporate Security Policies	Target Audience: Compliance
CONFIDENTIAL	Page 1 of 3

TruDiligence, LLC is hereinafter referred to as "the company."

1.0 Overview

The FCRA requires procedures to be in place for responding to a consumer dispute regarding the accuracy of a record. Trudiligence is in compliance with these regulations which are outlined in this policy.

2.0 Purpose

The policy is intended to provide guidelines to comply with FCRA's regulations regarding consumer disputes. Certain steps are required to verify the correct information is being released.

3.0 Scope

The scope of this policy covers all consumer disputes regarding the accuracy of records that are reported.

4.0 Policy

4.1 Consumer Disputes

FCRA sets forth detailed guidelines for handling consumer disputes regarding the accuracy of a record that was reported. In order for TruDiligence to comply with these regulations the following procedures are in place.

If the completeness or accuracy of any item of information contained in a consumer's file is disputed by the consumer and the consumer notifies the agency directly, or indirectly through a reseller, of such dispute, the agency shall, free of charge, conduct a reasonable reinvestigation to determine whether the disputed information is inaccurate and record the current status of the disputed information, or delete the item from the file before the end of the 30-day period beginning on the date on which TruDiligence receives the notice of the dispute from the consumer or reseller.

The 30-day period may be extended for not more than 15 additional days if TruDiligence receives information from the consumer during that 30-day period that is relevant to the reinvestigation.

Before the expiration of the 5-business-day period beginning on the date on which we receive notice of a dispute from any consumer or a reseller the agency shall provide notification of the dispute to any person who provided any item of information in dispute, at the address and in the manner established with the person. The notice shall include all relevant information regarding the dispute that the agency has received from the consumer or reseller.

Determination That Dispute Is Frivolous or Irrelevant
Trudiligence may terminate a reinvestigation of information disputed by a consumer if TruDiligence reasonably determines that the dispute by the consumer is frivolous or irrelevant, including by reason of a failure by a consumer to provide sufficient information to investigate the disputed information. Upon making any determination that a dispute is frivolous or irrelevant, TruDiligence shall notify the consumer of such determination not later than 5 business days after making such determination, by mail or, if authorized by the consumer for that purpose, by any other means available to the agency. A notice shall include the reasons for the determination and identification of any information required to investigate the disputed information, which may consist of a standardized form describing the general nature of such information.

In conducting any reinvestigation with respect to disputed information in the file of any consumer, TruDiligence shall review and consider all relevant information submitted by the consumer with respect to such disputed information.

If, after any reinvestigation of any information disputed by a consumer, an item of the information is found to be inaccurate or incomplete or cannot be verified, TruDiligence shall–

- promptly delete that item of information from the file of the consumer, or modify that item of information, as appropriate, based on the results of the reinvestigation; and
- promptly notify the furnisher of that information that the information has been modified or deleted from the file of the consumer.

If any information is deleted from a consumer's file, the information may not be reinserted in the file by TruDiligence unless the person who furnishes the information certifies that the information is complete and accurate.

If any information that has been deleted from a consumer's file is reinserted in the file, TruDiligence shall notify the consumer of the reinsertion in writing not later than 5 business days after the reinsertion or, if authorized by the consumer for that purpose, by any other means available to the agency.

TruDiligence shall provide written notice to a consumer of the results of a reinvestigation under this subsection not later than 5 business days after the completion of the reinvestigation, by mail or, if authorized by the consumer for that purpose, by other means available to the agency.

4.2 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 Compliance Officer and/or executive 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 if the policy is not followed.

7.0 Revision History

Revision 1.2 4/30/2008

TruDiligence, LLC

Criminal Database Searches	Created: 3/3/2009
Section of: Corporate Security Policies	Target Audience: Compliance
CONFIDENTIAL	Page 1 of 2

TruDiligence, LLC is hereinafter referred to as "the company."

1.0 Overview

Criminal Databases are often used to search for records on individuals. When such databases are used further research is required to verify the information that is being reported. Trudiligence maintains strict compliance efforts according to the requirements outlined by the FCRA which includes verifying any reportable records that are found in such databases not supported by the government.

2.0 Purpose

The policy is intended to provide guidelines to comply with FCRA and validate the accuracy of any reportable records found in a database that are not derived from a non-government owned or non-government sponsored/supported database.

3.0 Scope

The scope of this policy covers all database criminal record searches.

4.0 Policy

4.1 Database Criminal Record Searches

FCRA requires us to ensure and validate the accuracy of any public record reported back in our results. In order to comply and validate the accuracy of these searches reportable record found, will automatically be put through a direct county level criminal record search. This county level research will validate the information being reported back by the Database, thus maintaining the strictest FCRA compliance. The necessary county level searches will be automatically added to maintain compliance and billed accordingly.

4.2 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 Compliance Officer and/or executive 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 if the policy is not followed.

7.0 Revision History

Revision 1.2 4/30/2008

TruDiligence, LLC

Data Classification Policy	Created: 3/3/2009
Section of: Corporate Security Policies	Target Audience: Users, Technical
CONFIDENTIAL	Page 1 of 5

TruDiligence, LLC is hereinafter referred to as "the company."

1.0 Overview

Information assets are assets to the company just like physical property. In order to determine the value of the asset and how it should be handled, data must be classified according to its importance to company operations and the confidentiality of its contents. Once this has been determined, the company can take steps to ensure that data is treated appropriately.

2.0 Purpose

The purpose of this policy is to detail a method for classifying data and to specify how to handle this data once it has been classified.

3.0 Scope

The scope of this policy covers all company data stored on company-owned, company-leased, and otherwise company-provided systems and media, regardless of location. Also covered by the policy are hardcopies of company data, such as printouts, faxes, notes, etc.

4.0 Policy

4.1 Data Classification

Data residing on corporate systems must be continually evaluated and classified into the following categories:

1. Personal: includes user's personal data, emails, documents, etc. This policy excludes personal information, so no further guidelines apply.

2. Public: includes already-released marketing material, commonly known information, etc. There are no requirements for public information.

3. Operational: includes data for basic business operations, communications with vendors, employees, etc. (non-confidential). The majority of data will fall into this category.

4. Critical: any information deemed critical to business operations (often this data is operational or confidential as well). It is extremely important to identify critical data for security and backup purposes.

5. Confidential: any information deemed proprietary to the business. See the Confidential Data Policy for more detailed information about how to handle confidential data.

4.2 Data Storage

The following guidelines apply to storage of the different types of company data.

4.2.1 Personal

There are no requirements for personal information.

4.2.2 Public

There are no requirements for public information.

4.2.3 Operational

Operational data must be stored where the backup schedule is appropriate to the importance of the data, at the discretion of the user.

4.2.4 Critical

Critical data must be stored on a server that gets the most frequent backups (refer to the Backup Policy for additional information). System- or disk-level redundancy is required.

4.2.5 Confidential

Confidential information must be removed from desks, computer screens, and common areas unless it is currently in use. Confidential information should be stored under lock and key (or keycard/keypad), with the key, keycard, or code secured.

4.3 Data Transmission

The following guidelines apply to transmission of the different types of company data.

4.3.1 Personal

There are no requirements for personal information.

4.3.2 Public

There are no requirements for public information.

4.3.3 Operational
No specific requirements apply to transmission of Operational Data, however, as a general rule, the data should not be transmitted unless necessary for business purposes.

4.3.4 Critical
There are no requirements on transmission of critical data, unless the data in question is also considered operational or confidential, in which case the applicable policy statements would apply.

4.3.5 Confidential
Strong encryption must be used when transmitting confidential data, regardless of whether such transmission takes place inside or outside the company's network. Confidential data must not be left on voicemail systems, either inside or outside the company's network, or otherwise recorded.

4.4 Data Destruction
The following guidelines apply to the destruction of the different types of company data.

4.4.1 Personal
There are no requirements for personal information.

4.4.2 Public
There are no requirements for public information.

4.4.3 Operational
Cross-cut shredding is required for documents. Storage media should be appropriately sanitized/wiped or destroyed.

4.4.4 Critical
There are no requirements for the destruction of Critical Data, though shredding is encouraged. If the data in question is also considered operational or confidential, the applicable policy statements would apply.

4.4.5 Confidential
Confidential data must be destroyed in a manner that makes recovery of the information impossible. The following guidelines apply:

- Paper/documents: cross cut shredding is required.

- Storage media (CD's, DVD's): physical destruction is required.

- Hard Drives/Systems/Mobile Storage Media: physical destruction is required. If physical destruction is not possible, the IT Manager must be notified.

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 Manager and/or executive 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 will report such activities to the applicable authorities.

6.0 Definitions

Authentication A security method used to verify the identity of a user and authorize access to a system or network.

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

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.

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

Two-Factor Authentication A means of authenticating a user that utilizes two methods: something the user has, and something the user knows. Examples are smart cards, tokens, or biometrics, in combination with a password.

U.S. DoD Standards Stands for United States Department of Defense Standards. Standards

on data destruction detailed in DoD 5220.22-M. Most data wiping software packages provide an option for wiping to this standard.

7.0 Revision History

Revision 1.2 4/30/2008

TruDiligence, LLC

Encryption Policy	Created: 3/3/2009
Section of: Corporate Security Policies	Target Audience: Technical
CONFIDENTIAL	Page 1 of 4

TruDiligence, LLC 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:

- Whole disk encryption
- Encryption of partitions/files
- Encryption of disk drives
- Encryption of personal storage media/USB drives
- Encryption of backups

- Encryption of data generated by applications

2. Data while transmitted. This includes any data sent across the company network, or any data sent to or from a company-owned or company-provided system. Types of transmitted data that can be encrypted include:

- VPN tunnels
- Remote access sessions
- Web applications
- Email and email attachments
- Remote desktop access
- Communications with applications/databases

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
- Keys must be backed up
- Keys must be locked up
- Keys must never be transmitted in clear text
- Keys are confidential data
- Keys must not be shared
- Keys must not be stored on the same media as the encrypted information
- Physical key generation materials must be destroyed immediately upon generation.

- Keys must be used and changed in accordance with the password policy.

- When user encryption is employed, minimum key length is 10 characters.

- The company must perform background checks on the persons in charge of encryption keys.

- For secure storage the company should consider keys known in half by two people.

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 Manager and/or executive 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 are suspected the company will 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 1.2 4/30/2008

TruDiligence, LLC

Guest Access Policy	Created: 3/3/2009
Section of: Corporate Security Policies	Target Audience: Technical
CONFIDENTIAL	Page 1 of 3

TruDiligence, LLC is hereinafter referred to as "the company."

1.0 Overview

Guest access to the company's network is often necessary for customers, consultants, or vendors who are visiting the company's offices. This can be simply in the form of outbound Internet access, or the guest may require access to specific resources on the company's network. Guest access to the company's network must be tightly controlled.

2.0 Purpose

The company may wish to provide network access as a courtesy to guests wishing to access the Internet, or by necessity to visitors with a business need to access the company's resources. This policy outlines the company's procedures for securing guest access.

3.0 Scope

The scope of this policy includes any visitor to the company wishing to access the network or Internet through the company's infrastructure, and covers both wired and wireless connections. This scope excludes guests accessing wireless broadband accounts directly through a cellular carrier or third party where the traffic does not traverse the company's network.

4.0 Policy

4.1 Granting Guest Access

Guest access will be provided on a case-by-case basis to any person who can demonstrate a reasonable business need to access the network, or access the Internet from the company network.

4.1.1 AUP Acceptance

Guests must agree to and sign the company's Acceptable Use Policy (AUP) before being granted access.

4.1.2 Approval

Guest need for access will be evaluated and provided on a case-by-case basis. This

should involve management approval if the request is non-standard.

4.1.3 Account Use

Guest accounts, if offered, are only to be used by guests. Users with network accounts must use their accounts for network access. Guest accounts must be set up for each guest accessing the company's network. Guest accounts must have specific expiration dates that correlate to the business need for the individual guest's access. The account expiration date is not to exceed thirty days.

4.1.4 Security of Guest Machines

Guest machines must be audited by the Information Technology department before being allowed to access the network. The company should ensure that that the Network Access Policy will be adhered to, which may involve a virus/malware scan prior to being granted access.

4.2 Guest Access Infrastructure Requirements

Best practices dictate that guest access be kept separate, either logically or physically, from the corporate network, since guests have typically not undergone the same amount of scrutiny as the company's employees. This must be weighed, however, with the costs and technical issues that come with providing such separation. At this time the company does not provide any specific requirements for guest access infrastructure. Guest access should be provided prudently and monitored for appropriateness of use.

4.3 Restrictions on Guest Access

Guest access will be restricted to the minimum amount necessary. Depending on the guest needing access, this can often be limited to outbound Internet access only. The company will evaluate the need of each guest and provide further access if there is a business need to do so.

4.4 Monitoring of Guest Access

Since guests are not employees of the company they are not considered trusted users. As such, the company will monitor guest access to ensure that the company's interests are protected and the Acceptable Use Policy is being adhered to.

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 Manager and/or executive team. Violations may result in termination or restriction of the guest's access. Where illegal activities are suspected, Company will report such activities to the applicable authorities.

6.0 Definitions

Account A combination of username and password that allows access to computer or network resources.

Guest A visitor to the company premises who is not an employee.

7.0 Revision History

Revision 1.2 4/30/2008

TruDiligence, LLC

Guest Access Policy	Created: 3/3/2009
Section of: Corporate Security Policies	Target Audience: Technical
CONFIDENTIAL	Page 1 of 3

TruDiligence, LLC is hereinafter referred to as "the company."

1.0 Overview

Guest access to the company's network is often necessary for customers, consultants, or vendors who are visiting the company's offices. This can be simply in the form of outbound Internet access, or the guest may require access to specific resources on the company's network. Guest access to the company's network must be tightly controlled.

2.0 Purpose

The company may wish to provide network access as a courtesy to guests wishing to access the Internet, or by necessity to visitors with a business need to access the company's resources. This policy outlines the company's procedures for securing guest access.

3.0 Scope

The scope of this policy includes any visitor to the company wishing to access the network or Internet through the company's infrastructure, and covers both wired and wireless connections. This scope excludes guests accessing wireless broadband accounts directly through a cellular carrier or third party where the traffic does not traverse the company's network.

4.0 Policy

4.1 Granting Guest Access

Guest access will be provided on a case-by-case basis to any person who can demonstrate a reasonable business need to access the network, or access the Internet from the company network.

4.1.1 AUP Acceptance

Guests must agree to and sign the company's Acceptable Use Policy (AUP) before being granted access.

4.1.2 Approval

Guest need for access will be evaluated and provided on a case-by-case basis. This

should involve management approval if the request is non-standard.

4.1.3 Account Use

Guest accounts, if offered, are only to be used by guests. Users with network accounts must use their accounts for network access. Guest accounts must be set up for each guest accessing the company's network. Guest accounts must have specific expiration dates that correlate to the business need for the individual guest's access. The account expiration date is not to exceed thirty days.

4.1.4 Security of Guest Machines

Guest machines must be audited by the Information Technology department before being allowed to access the network. The company should ensure that that the Network Access Policy will be adhered to, which may involve a virus/malware scan prior to being granted access.

4.2 Guest Access Infrastructure Requirements

Best practices dictate that guest access be kept separate, either logically or physically, from the corporate network, since guests have typically not undergone the same amount of scrutiny as the company's employees. This must be weighed, however, with the costs and technical issues that come with providing such separation. At this time the company does not provide any specific requirements for guest access infrastructure. Guest access should be provided prudently and monitored for appropriateness of use.

4.3 Restrictions on Guest Access

Guest access will be restricted to the minimum amount necessary. Depending on the guest needing access, this can often be limited to outbound Internet access only. The company will evaluate the need of each guest and provide further access if there is a business need to do so.

4.4 Monitoring of Guest Access

Since guests are not employees of the company they are not considered trusted users. As such, the company will monitor guest access to ensure that the company's interests are protected and the Acceptable Use Policy is being adhered to.

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 Manager and/or executive team. Violations may result in termination or restriction of the guest's access. Where illegal activities are suspected, Company will report such activities to the applicable authorities.

6.0 Definitions

Account A combination of username and password that allows access to computer or network resources.

Guest A visitor to the company premises who is not an employee.

7.0 Revision History

Revision 1.2 4/30/2008

TruDiligence, LLC

Incident Response Policy	Created: 3/3/2009
Section of: Corporate Security Policies	Target Audience: Technical
CONFIDENTIAL	Page 1 of 6

TruDiligence, LLC is hereinafter referred to as "the company."

1.0 Overview

A security incident can come in many forms: a malicious attacker gaining access to the network, a virus or other malware infecting computers, or even a stolen laptop containing confidential data. A well-thought-out Incident Response Policy is critical to successful recovery from an incident. This policy covers all incidents that may affect the security and integrity of the company's information assets, and outlines steps to take in the event of such an incident.

2.0 Purpose

This policy is intended to ensure that the company is prepared if a security incident were to occur. It details exactly what must occur if an incident is suspected, covering both electronic and physical security incidents. Note that this policy is not intended to provide a substitute for legal advice, and approaches the topic from a security practices perspective.

3.0 Scope

The scope of this policy covers all information assets owned or provided by the company, whether they reside on the corporate network or elsewhere.

4.0 Policy

4.1 Types of Incidents

A security incident, as it relates to the company's information assets, can take one of two forms. For the purposes of this policy a security incident is defined as one of the following:

- Electronic: This type of incident can range from an attacker or user accessing the network for unauthorized/malicious purposes, to a virus outbreak, to a suspected Trojan or malware infection.

- Physical: A physical IT security incident involves the loss or theft of a laptop, mobile device, PDA/Smartphone, portable storage device, or other digital apparatus that may contain company information.

4.2 Preparation

Work done prior to a security incident is arguably more important than work done after an incident is discovered. The most important preparation work, obviously, is maintaining good security controls that will prevent or limit damage in the event of an incident. This includes technical tools such as firewalls, intrusion detection systems, authentication, and encryption; and non-technical tools such as good physical security for laptops and mobile devices.

Additionally, prior to an incident, the company must ensure that the following is clear to IT personnel:

- What actions to take when an incident is suspected.
- Who is responsible for responding to an incident.

The company should strongly consider having discussions with an IT Security company that offers incident response services before such an incident occurs in order to prepare an emergency service contract. This will ensure that high-end resources are quickly available during an incident.

Finally, the company should review any industry or governmental regulations that dictate how it must respond to a security incident (specifically, loss of customer data), and ensure that its incident response plans adhere to these regulations.

4.3 Confidentiality

All information related to an electronic or physical security incident must be treated as confidential information until the incident is fully contained. This will serve both to protect employees' reputations (if an incident is due to an error, negligence, or carelessness), and to control the release of information to the media and/or customers.

4.4 Electronic Incidents

When an electronic incident is suspected, the company's goal is to recover as quickly as possible, limit the damage done, secure the network, and preserve evidence of the incident. The following steps should be taken in order:

1. Before an incident occurs, the company must work out a response scenario with a qualified IT Security consultant that includes emergency access to high-end expertise.

2. Remove the compromised device from the network by unplugging or disabling network connection. Do not power down the machine.

3. Disable the compromised account(s) as appropriate.

4. Report the incident to the IT Manager.

5. Physically secure the compromised system.

6. Contact the security consultant for emergency response. If prosecution of the incident is desired, chain-of-custody and preservation of evidence are critical.

7. Create a detailed event log documenting each step taken during this process.

8. Determine how the attacker gained access and disable this access.

9. Rebuild the system using new hardware.

10. Restore any needed data from the last known good backup and put the system back online.

11. Take actions, as possible, to ensure that the vulnerability (or similar vulnerabilities) will not reappear.

12. Notify applicable authorities if prosecution is desired and possible based on the evidence collected.

13. Reflect on the incident. What can be learned? How did the Incident Response team perform? Was the policy adequate? What could be done differently?

14. Perform a vulnerability assessment as a way to spot any other vulnerabilities before they can be exploited.

4.5 Physical Incidents

Physical security incidents are challenging, since often the only actions that can be taken to mitigate the incident must be done in advance. This makes preparation critical. One of the best ways to prepare is to mandate the use of strong encryption to secure data on mobile devices. Applicable polices, such as those covering encryption and confidential data, should be reviewed.

Physical security incidents are most likely the result of a random theft of inadvertent loss by a

user, but they must be treated as if they were targeted at the company.

The company must assume that such a loss will occur at some point, and periodically survey a random sampling of laptops and mobile devices to determine the risk if one were to be lost or stolen.

4.5.1 Response

Establish the severity of the incident by determining the data stored on the missing device. This can often be done by referring to a recent backup of the device. Two important questions must be answered:

1. Was confidential data involved?
    a. If not, refer to "Loss Contained" below.
    b. If confidential data was involved, refer to "Data Loss Suspected" below.

2. Was strong encryption used?
    a. If strong encryption was used, refer to "Loss Contained" below.
    b. If not, refer to "Data Loss Suspected" below.

4.5.2 Loss Contained

First, change any usernames, passwords, account information, WEP/WPA keys, passphrases, etc., that were stored on the system. Notify the IT Manager. Replace the lost hardware and restore data from the last backup. Notify the applicable authorities if a theft has occurred.

4.5.3 Data Loss Suspected

First, notify the executive team, legal counsel, and/or public relations group so that each team can evaluate and prepare a response in their area.

Change any usernames, passwords, account information, WEP/WPA keys, passphrases, etc., that were stored on the system. Replace the lost hardware and restore data from the last backup. Notify the applicable authorities as needed if a theft has occurred and follow disclosure guidelines specified in the notification section.

Review procedures to ensure that risk of future incidents is reduced by implementing stronger physical security controls.

4.6 Notification

If an electronic or physical security incident is suspected to have resulted in the loss of

third-party/customer data, notification of the public or affected entities should occur. First this must be discussed with executive team and legal counsel to determine an appropriate course of action. If notification is deemed an appropriate, it should occur in an organized and consistent manner.

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 Manager and/or executive team. Where crimes are suspected, the appropriate authorities will be notified. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment.

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.

Malware Short for "malicious software." A software application designed with malicious intent. Viruses and Trojans are common examples of malware.

Mobile Device A portable device that can be used for certain applications and data storage. Examples are PDAs or Smartphones.

PDA Stands for Personal Digital Assistant. A portable device that stores and organizes personal information, such as contact information, calendar, and notes.

Smartphone A mobile telephone that offers additional applications, such as PDA functions and email.

Trojan Also called a "Trojan Horse." An application that is disguised as something innocuous or legitimate, but harbors a malicious payload. Trojans can be used to covertly and remotely gain access to a computer, log keystrokes, or perform other malicious or destructive acts.

Virus Also called a "Computer Virus." A replicating application that attaches itself to other data, infecting files similar to how a virus infects cells. Viruses can be spread through email or via network-connected computers and file systems.

WEP Stands for Wired Equivalency Privacy. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. WEP can be cryptographically broken with relative ease.

WPA Stands for WiFi Protected Access. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. Newer and considered more secure than WEP.

7.0 Revision History

Revision 1.2 4/30/2008

TruDiligence, LLC

Mobile Device Policy	Created: 3/3/2009
Section of: Corporate Security Policies	Target Audience: Users, Technical
CONFIDENTIAL	Page 1 of 4

TruDiligence, LLC is hereinafter referred to as "the company."

1.0 Overview

Generally speaking, a more mobile workforce is a more flexible and productive workforce. For this reason, business use of mobile devices is growing. However, as these devices become vital tools to the workforce, more and more sensitive data is stored on them, and thus the risk associated with their use is growing. Special consideration must be given to the security of mobile devices.

2.0 Purpose

The purpose of this policy is to specify company standards for the use and security of mobile devices.

3.0 Scope

This policy applies to company data as it relates to mobile devices that are capable of storing such data, including, but not limited to, laptops, notebooks, PDAs, smart phones, and USB drives. Since the policy covers the data itself, ownership of the mobile device is irrelevant. This policy covers any mobile device capable of coming into contact with company data.

4.0 Policy

4.1 Physical Security

By nature, a mobile device is more susceptible to loss or theft than a non-mobile system. The company should carefully consider the physical security of its mobile devices and take appropriate protective measures, including the following:

- Laptop locks and cables can be used to secure laptops when in the office or other fixed locations.

- Mobile devices should be kept out of sight when not in use.

- Care should be given when using or transporting mobile devices in busy areas.

- As a general rule, mobile devices must not be stored in cars. If the situation leaves no other viable alternatives, the device must be stored in the trunk, with the interior trunk release locked; or in a lockable compartment such as a glove box.

- The company should evaluate the data that will be stored on mobile devices and consider remote wipe/remote delete technology. This technology allows a user or administrator to make the data on the mobile device unrecoverable.

- The company should continue to monitor the market for physical security products for mobile devices, as it is constantly evolving.

4.2 Data Security

If a mobile device is lost or stolen, the data security controls that were implemented on the device are the last line of defense for protecting company data. The following sections specify the company's requirements for data security as it relates to mobile devices.

4.2.1 Laptops

At a minimum, company data must be stored on an encrypted partition. Whole disk encryption should be considered if the data is especially sensitive. Laptops must require a username and password or biometrics for login.

4.2.2 PDAs/Smart Phones

Use of encryption is not required on PDAs/smart phones but it encouraged if data stored on the device is especially sensitive. PDAs/smart phones must require a password for login.

4.2.3 Mobile Storage Media

This section covers any USB drive, flash drive, memory stick or other personal data storage media. Storing company data on such devices is not permitted under any circumstance.

4.2.4 Portable Media Players

No company data can be stored on personal media players.

4.2.5 Other Mobile Devices

Unless specifically addressed by this policy, storing company data on other mobile devices, or connecting such devices to company systems, is expressly prohibited.

Questions or requests for clarification on what is and is not covered should be directed to the IT Manager.

4.3 Connecting to Unsecured Networks

Users must not connect to any outside network without a secure, up-to-date software firewall configured on the mobile computer. Examples of unsecured networks would typically, but not always, relate to Internet access, such as access provided from a home network, access provided by a hotel, an open or for-pay wireless hotspot, a convention network, or any other network not under direct control of the company.

4.4 General Guidelines

The following guidelines apply to the use of mobile devices:

- Loss, Theft, or other security incident related to a company-provided mobile device must be reported promptly.

- Confidential data should not be stored on mobile devices unless it is absolutely necessary. If confidential data is stored on a mobile device it must be appropriately secured and comply with the Confidential Data policy.

- Data stored on mobile devices must be securely disposed of in accordance with the Data Classification Policy.

- Users are not to store company data on non-company-provided mobile equipment. This does not include simple contact information, such as phone numbers and email addresses, stored in an address book on a personal phone or PDA.

4.5 Audits

The company must conduct periodic reviews to ensure policy compliance. A sampling of mobile devices should be taken and audited against this policy on a periodic basis.

4.6 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 Manager and/or executive 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 is suspected, the company will 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.

Mobile Devices A portable device that can be used for certain applications and data storage. Examples are PDAs or Smartphones.

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.

PDA Stands for Personal Digital Assistant. A portable device that stores and organizes personal information, such as contact information, calendar, and notes.

Portable Media Player A mobile entertainment device used to play audio and video files. Examples are mp3 players and video players.

Smartphone A mobile telephone that offers additional applications, such as PDA functions and email.

7.0 Revision History

Revision 1.2 4/30/2008

TruDiligence, LLC

Network Access and Authentication Policy	Created: 3/3/2009
Section of: Corporate Security Policies	Target Audience: Technical
CONFIDENTIAL	Page 1 of 5

TruDiligence, LLC is hereinafter referred to as "the company."

1.0 Overview

Any user accessing the company's computer systems has the ability to affect the security of all users of the system. A sound network access policy provides consistent application of authentication and access standards across the company.

2.0 Purpose

The purpose of this policy is to describe what steps must be taken to ensure that users connecting to the corporate network are authenticated in an appropriate manner, in compliance with company standards, and are given the least amount of access required to perform their job function.

3.0 Scope

The scope of this policy includes all users who have access to company-owned or company-provided computers or require access to the corporate network and/or systems.

4.0 Policy

4.1 Account Setup

During initial account setup, certain checks must be performed in order to ensure the integrity of the process. The following policies apply to account setup:

- Positive ID and coordination with Human Resources is required.
- Users will be granted least amount of network access required to perform his or her job function.
- Users will be granted access only if he or she accepts the Acceptable Use Policy.
- Access to the network will be granted in accordance with the Acceptable Use Policy.

4.2 Account Use

Network accounts must be implemented in a standard fashion and utilized consistently across the organization. The following policies apply to account use:

- Accounts must be created using a standard format (i.e., firstname-lastname, or firstinitial-lastname, etc.)

- Accounts must be password protected (refer to the Password Policy for more detailed information).

- Accounts must be for individuals only. Account sharing and group accounts are not permitted.

- User accounts must not be given administrator or `root' access unless this is necessary to perform his or her job function.

- Occasionally guests will have a legitimate business need for access to the corporate network. When a reasonable need is demonstrated, temporary guest access is allowed. This access, however, must be severely restricted to only those resources that the guest needs at that time, and disabled when the guest's work is completed.

4.3 Account Termination

When managing network and user accounts, it is important to stay in communication with the Human Resources department so that when an employee no longer works at the company, that employee's account can be disabled. Human Resources must create a process to notify the IT Manager in the event of a staffing change, which includes employment termination, employment suspension, or a change of job function (promotion, demotion, suspension, etc.).

4.4 Authentication

User machines must be configured to request authentication against the domain at startup. If the domain is not available or authentication for some reason cannot occur, then the machine should not be permitted to access the network.

4.5 Use of Passwords

When accessing the network locally, username and password is an acceptable means of authentication.

4.6 Remote Network Access

Remote access to the network can be provided for convenience to users but this comes at some risk to security. For that reason, the company encourages additional scrutiny of users remotely accessing the network. The company's standards dictate that username and password is an acceptable means of authentication. Remote access must adhere to the Remote Access Policy.

4.7 Screensaver Passwords

Screensaver passwords offer an easy way to strengthen security by removing the opportunity for a malicious user, curious employee, or intruder to access network resources through an idle computer. For this reason screensaver passwords are encouraged.

4.8 Minimum Configuration for Access

Users must adhere to corporate standards with regard to antivirus software and patch levels on their machines. Users must not be permitted network access if these standards are not met. This policy will be enforced with product that provides network admission control.

4.9 Encryption

Authentication credentials must be encrypted during transmission across any network, whether the transmission occurs internal to the company network or across a public network such as the Internet.

4.10 Failed Logons

Repeated logon failures can indicate an attempt to `crack' a password and surreptitiously access a network account. In order to guard against password-guessing and brute-force attempts, the company must lock a user's account after 3 unsuccessful logins. This can be implemented as a time-based lockout or require a manual reset, at the discretion of the IT Manager.

In order to protect against account guessing, when logon failures occur the error message transmitted to the user must not indicate specifically whether the account name or password were incorrect. The error can be as simple as "the username and/or password you supplied were incorrect."

4.11 Non-Business Hours

While some security can be gained by removing account access capabilities during non-business hours, the company does not mandate time-of-day lockouts. This may be either to encourage working remotely, or because the company's business requires all-hours access.

4.12 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 Manager and/or executive team, and should be validated through periodic audit. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment.

6.0 Definitions

Antivirus Software An application used to protect a computer from viruses, typically through real time defenses and periodic scanning. Antivirus software has evolved to cover other threats, including Trojans, spyware, and other malware.

Authentication A security method used to verify the identity of a user and authorize access to a system or network.

Biometrics The process of using a person's unique physical characteristics to prove that person's identity. Commonly used are fingerprints, retinal patterns, and hand geometry.

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.

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.

Smart Card A plastic card containing a computer chip capable of storing information, typically to prove the identity of the user. A card-reader is required to access the information.

Token A small hardware device used to access a computer or network. Tokens are typically in the form of an electronic card or key fob with a regularly changing code on its display.

7.0 Revision History

Revision 1.2 4/30/2008

TruDiligence, LLC

Network Security Policy	Created: 3/3/2009
Section of: Corporate Security Policies	Target Audience: Technical
CONFIDENTIAL	Page 1 of 13

TruDiligence, LLC is hereinafter referred to as "the company."

1.0 Overview

The company wishes to provide a secure network infrastructure in order to protect the integrity of corporate data and mitigate risk of a security incident. While security policies typically avoid providing overly technical guidelines, this policy is necessarily a more technical document than most.

2.0 Purpose

The purpose of this policy is to establish the technical guidelines for IT security, and to communicate the controls necessary for a secure network infrastructure. The network security policy will provide the practical mechanisms to support the company's comprehensive set of security policies. However, this policy purposely avoids being overly-specific in order to provide some latitude in implementation and management strategies.

3.0 Scope

This policy covers all IT systems and devices that comprise the corporate network or that are otherwise controlled by the company.

4.0 Policy

4.1 Network Device Passwords

A compromised password on a network device could have devastating, network-wide consequences. Passwords that are used to secure these devices, such as routers, switches, and servers, must be held to higher standards than standard user-level or desktop system passwords.

4.1.1 Password Construction

The following statements apply to the construction of passwords for network devices:

- Passwords should be at least 6 characters
- Passwords should be comprised of a mix of letters, numbers and special

characters (punctuation marks and symbols)

- Passwords should be comprised of a mix of upper and lower case characters

- Passwords should not be comprised of, or otherwise utilize, words that can be found in a dictionary

- Passwords should not be comprised of an obvious keyboard sequence (i.e., qwerty)

- Passwords should not include "guessable" data such as personal information like birthdays, addresses, phone numbers, locations, etc.

4.1.2 Failed Logons

Repeated logon failures can indicate an attempt to `crack' a password and surreptitiously access a network account. In order to guard against password-guessing and brute-force attempts, the company must lock a user's account after 3 unsuccessful logins. This can be implemented as a time-based lockout or require a manual reset, at the discretion of the IT Manager.

In order to protect against account guessing, when logon failures occur the error message transmitted to the user must not indicate specifically whether the account name or password were incorrect. The error can be as simple as "the username and/or password you supplied were incorrect."

4.1.3 Change Requirements

Passwords must be changed according to the company's Password Policy. Additionally, the following requirements apply to changing network device passwords:

- If any network device password is suspected to have been compromised, all network device passwords must be changed immediately.

- If a company network or system administrator leaves the company, all passwords to which the administrator could have had access must be changed immediately. This statement also applies to any consultant or contractor who has access to administrative passwords.

- Vendor default passwords must be changed when new devices are put into service.

4.1.4 Password Policy Enforcement

Where passwords are used an application must be implemented that enforces the company's password policies on construction, changes, re-use, lockout, etc.

4.1.5 Administrative Password Guidelines

As a general rule, administrative (also known as "root") access to systems should be limited to only those who have a legitimate business need for this type of access. This is particularly important for network devices, since administrative changes can have a major effect on the network, and, as such, network security. Additionally, administrative access to network devices should be logged.

4.2 Logging

The logging of certain events is an important component of good network management practices. Logging needs vary depending on the type of network system, and the type of data the system holds. The following sections detail the company's requirements for logging and log review.

4.2.1 Application Servers

Logs from application servers are of interest since these servers often allow connections from a large number of internal and/or external sources. These devices are often integral to smooth business operations.

Examples: Web, email, database servers

Requirement: At a minimum, logging of errors, faults, and login failures is required. Additional logging is encouraged as deemed necessary. No passwords should be contained in logs.

4.2.2 Network Devices

Logs from network devices are of interest since these devices control all network traffic, and can have a huge impact on the company's security.

Examples: Firewalls, network switches, routers

Requirement: At a minimum, logging of errors, faults, and login failures is required. Additional logging is encouraged as deemed necessary. No passwords should be contained in logs.

4.2.3 Critical Devices

Critical devices are any systems that are critically important to business operations. These systems may also fall under other categories above - in any cases where this occurs, this section shall supersede.

Examples: File servers, lab or manufacturing machines, systems storing intellectual property

Requirements: At a minimum, logging of errors, faults, and login failures is required. Additional logging is encouraged as deemed necessary. No passwords should be contained in logs.

4.2.4 Log Management

Logs should be retained in accordance with the company's Retention Policy. Unless otherwise determined by the IT manager, logs should be considered operational data.

4.3 Firewalls

Firewalls are arguably the most important component of a sound security strategy. Internet connections and other unsecured networks must be separated from the company network through the use of a firewall.

4.3.1 Configuration

The following statements apply to the company's implementation of firewall technology:

- Firewalls must provide secure administrative access (through the use of encryption) with management access limited, if possible, to only networks where management connections would be expected to originate.

- No unnecessary services or applications should be enabled on firewalls. The company should use `hardened' systems for firewall platforms, or appliances.

- Clocks on firewalls should be synchronized with the company's other networking hardware using NTP or another means. Among other benefits, this will aid in problem resolution and security incident investigation.

- The firewall ruleset must be documented and audited quarterly. Audits must cover each rule, what it is for, if it is still necessary, and if it can be improved.

- For its own protection, the firewall ruleset must include a "stealth rule," which forbids connections to the firewall itself.

- The firewall must log dropped or rejected packets.

4.3.2 Outbound Traffic Filtering

Firewalls are often configured to block only inbound connections from external sources; however, by filtering outbound connections from the network, security can be greatly improved. This practice is also referred to as "Egress Traffic Filtering."

Blocking outbound traffic prevents users from accessing unnecessary, and many times, dangerous services. By specifying exactly what outbound traffic to allow, all other outbound traffic is blocked. This type of filtering would block root kits, viruses, and other malicious tools if a host were to become compromised. This will also prevent remote desktops from accessing the internal network.

The company encourages outbound filtering if possible, but it is not required. If filtering is deemed possible, only the following known "good" services should be permitted outbound from the network: 21, 22, 23, 25, 53, 80, 110, 443, and 995.

4.4 Networking Hardware

Networking hardware, such as routers, switches, hubs, bridges, and access points, should be implemented in a consistent manner. The following statements apply to the company's implementation of networking hardware:

- Networking hardware must provide secure administrative access (through the use of encryption) with management access limited, if possible, to only networks where management connections would be expected to originate.

- Clocks on all network hardware should be synchronized using NTP or another means. Among other benefits, this will aid in problem resolution and security incident investigation.

- If possible for the application, switches are preferred over hubs. When using switches the company should use VLANs to separate networks if it is reasonable and possible to do so.

- Access control lists should be implemented on network devices that prohibit direct connections to the devices. Exceptions to this are management connections that can be limited to known sources.

- Unused services and ports should be disabled on networking hardware.

• Access to administrative ports on networking hardware should be restricted to known management hosts and otherwise blocked with a firewall or access control list.

4.5 Network Servers

Servers typically accept connections from a number of sources, both internal and external. As a general rule, the more sources that connect to a system, the more risk that is associated with that system, so it is particularly important to secure network servers. The following statements apply to the company's use of network servers:

• Unnecessary files, services, and ports should be removed or blocked. If possible, follow a server-hardening guide, which is available from the leading operating system manufacturers.

• Network servers, even those meant to accept public connections, must be protected by a firewall or access control list.

• If possible, a standard installation process should be developed for the company's network servers. This will provide consistency across servers no matter what employee or contractor handles the installation.

• Clocks on network servers should be synchronized with the company's other networking hardware using NTP or another means. Among other benefits, this will aid in problem resolution and security incident investigation.

4.6 Intrusion Detection/Intrusion Prevention

Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) technology can be useful in network monitoring and security. The tools differ in that an IDS alerts to suspicious activity whereas an IPS blocks the activity. When tuned correctly, IDSs are useful but can generate a large amount of data that must be evaluated for the system to be of any use. IPSs automatically take action when they see suspicious events, which can be both good and bad, since legitimate network traffic can be blocked along with malicious traffic.

The company neither requires nor prohibits the use of IDS or IPS systems. The decision to use IDS/IPS systems is left to the discretion of the IT Manager.

4.7 Security Testing

Security testing, also known as a vulnerability assessment, a security audit, or penetration testing, is an important part of maintaining the company's network security. Security testing can be provided by IT Staff members, but is often more effective when performed by a third party

with no connection to the company's day-to-day Information Technology activities. The following sections detail the company's requirements for security testing.

4.7.1 Internal Security Testing

Internal security testing does not necessarily refer to testing of the internal network, but rather testing performed by members of the company's IT team. Internal testing should not replace external testing; however, when external testing is not practical for any reason, or as a supplement to external testing, internal testing can be helpful in assessing the security of the network.

Internal security testing is allowable, but only by employees whose job functions are to assess security, and only with permission of the IT Manager. Internal testing should have no measurable negative impact on the company's systems or network performance.

4.7.2 External Security Testing

External security testing, which is testing by a third party entity, is an excellent way to audit the company's security controls. The IT Manager must determine to what extent this testing should be performed, and what systems/applications it should cover.

External testing must not negatively affect network performance during business hours or network security at any time.

As a rule, "penetration testing," which is the active exploitation of company vulnerabilities, should be discouraged. If penetration testing is performed, it must not negatively impact company systems or data.

The company encourages external security testing, but does not provide rigid guidelines regarding at what intervals the testing should occur. Testing should be performed as often as is necessary, as determined by the IT Manager.

4.8 Disposal of Information Technology Assets

IT assets, such as network servers and routers, often contain sensitive data about the company's network communications. When such assets are decommissioned, the following guidelines must be followed:

- Any asset tags or stickers that identify the company must be removed before disposal.

- Any configuration information must be removed by deletion or, if applicable, resetting the device to factory defaults.

• At a minimum, data wiping must be used. Simply reformatting a drive or deleting data does not make the data unrecoverable. If wiping is used, the company must follow DoD (U.S. Department of Defense) guidelines for data wiping. Alternatively, the company has the option of physically destroying the data storage mechanism from the device (such as its hard drive or solid state memory).

4.9 Network Compartmentalization

Good network design is integral to network security. By implementing network compartmentalization, which is separating the network into different segments, the company will reduce its network-wide risk from an attack or virus outbreak. Further, security can be increased if traffic must traverse additional enforcement/inspection points. The company requires the following with regard to network compartmentalization:

4.9.1 Higher Risk Networks

Examples: Guest network, wireless network

Requirements: Segmentation of higher risk networks from the company's internal network is encouraged but not required.

4.9.2 Externally-Accessible Systems

Examples: Email servers, web servers

Requirements: Segmentation of externally-accessible systems from the company's internal network is encouraged but not required.

4.9.3 Internal Networks

Examples: Sales, Finance, Human Resources

Requirements: Segmentation of internal networks from one another can improve security as well as reduce chances that a user will access data that he or she has no right to access. The company encourages, but does not require, such segmentation.

4.10 Network Documentation

Network documentation, specifically as it relates to security, is important for efficient and successful network management. Further, the process of regularly documenting the network ensures that the company's IT Staff has a firm understanding of the network architecture at any given time. The intangible benefits of this are immeasurable.

Network documentation should include:

- Network diagram(s)
- System configurations
- Firewall ruleset
- IP Addresses
- Access Control Lists

The company encourages network documentation, but does not require it.

4.11 Antivirus/Ant-Malware

Computer viruses and malware are pressing concerns in today's threat landscape. If a machine or network is not properly protected, a virus outbreak can have devastating effects on the machine, the network, and the entire company. The company provides the following guidelines on the use of antivirus/anti-malware software:

- All company-provided user workstations must have antivirus/anti-malware software installed.
- Workstation software must maintain a current "subscription" to receive patches and virus signature/definition file updates.
- Patches, updates, and antivirus signature file updates must be installed in a timely manner, either automatically or manually.

4.12 Software Use Policy

Software applications can create risk in a number of ways, and thus certain aspects of software use must be covered by this policy. The company provides the following requirements for the use of software applications:

- Only legally licensed software may be used. Licenses for the company's software must be stored in a secure location.

- Open source and/or public domain software can only be used with the permission of the IT Manager.

- Software should be kept reasonably up-to-date by installing new patches and releases from the manufacturer.

- Vulnerability alerts should be monitored for all software products that the company uses. Any patches that fix vulnerabilities or security holes must be installed expediently.

4.13 Maintenance Windows and Scheduled Downtime

Certain tasks require that network devices be taken offline, either for a simple re-boot, an upgrade, or other maintenance. When this occurs, the IT Staff should make every effort to perform the tasks at times when they will have the least impact on network users.

4.14 Change Management

Documenting changes to network devices is a good management practice and can help speed resolution in the event of an incident. The IT Staff should make a reasonable effort to document hardware and/or configuration changes to network devices in a "change log." If possible, network devices should bare a sticker or tag indicating essential information, such as the device name, IP address, Mac address, asset information, and any additional data that may be helpful, such as information about cabling.

4.15 Suspected Security Incidents

When a security incident is suspected that may impact a network device, the IT Staff should refer to the company's Incident Response policy for guidance.

4.16 Redundancy

Redundancy can be implemented on many levels, from redundancy of individual components to full site-redundancy. As a general rule, the more redundancy implemented, the higher the availability of the device or network, and the higher the associated cost. The company wishes to provide the IT Manager with latitude to determine the appropriate level of redundancy for critical systems and network devices. Redundancy should be implemented where it is needed, and should include some or all of the following:

- Hard drive redundancy, such as mirroring or RAID

- Server level redundancy, such as clustering or high availability

- Component level redundancy, such as redundant power supplies or redundant NICs
- Keeping hot or cold spares onsite

4.17 Manufacturer Support Contracts

Outdated products can result in a serious security breach. When purchasing critical hardware or software, the company should consider purchasing a maintenance plan, support agreement, or software subscription that will allow the company to receive updates to the software and/or firmware for a specified period of time. If such a plan is purchased, it should meet the following standards:

Hardware: The arrangement should allow for repair/replacement of the device within an acceptable time period, as determined by the IT Manager, as well as firmware or embedded software updates.

Software: The arrangement should allow for updates, upgrades, and hotfixes for a specified period of time.

4.18 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 Manager and/or executive 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.

6.0 Definitions

ACL A list that defines the permissions for use of, and restricts access to, network resources. This is typically done by port and IP address.

Antivirus Software An application used to protect a computer from viruses, typically through real time defenses and periodic scanning. Antivirus software has evolved to cover other threats,

including Trojans, spyware, and other malware.

Firewall A security system that secures the network by enforcing boundaries between secure and insecure areas. Firewalls are often implemented at the network perimeter as well as in high-security or high-risk areas.

Hub A network device that is used to connect multiple devices together on a network.

IDS Stands for Intrusion Detection System. A network monitoring system that detects and alerts to suspicious activities.

IPS Stands for Intrusion Prevention System. A networking monitoring system that detects and automatically blocks suspicious activities.

NTP Stands for Network Time Protocol. A protocol used to synchronize the clocks on networked devices.

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

RAID Stands for Redundant Array of Inexpensive Disks. A storage system that spreads data across multiple hard drives, reducing or eliminating the impact of the failure of any one drive.

Switch A network device that is used to connect devices together on a network. Differs from a hub by segmenting computers and sending data to only the device for which that data was intended.

U.S. DoD Standards Stands for United States Department of Defense Standards. Standards on data destruction detailed in DoD 5220.22M. Most data wiping software packages provide an option for wiping to this standard.

VLAN Stands for Virtual LAN (Local Area Network). A logical grouping of devices within a network that act as if they are on the same physical LAN segment.

Virus Also called a "Computer Virus." A replicating application that attaches itself to other data, infecting files similar to how a virus infects cells. Viruses can be spread through email or via network-connected computers and file systems.

7.0 Revision History

Revision 1.2 4/30/2008

TruDiligence, LLC

Outsourcing Policy	Created: 3/3/2009
Section of: Corporate Security Policies	Target Audience: Technical
CONFIDENTIAL	Page 1 of 4

TruDiligence, LLC is hereinafter referred to as "the company."

1.0 Overview

Outsourcing is a logical practice when specialized expertise is required, which happens frequently in the field of Information Technology (IT). Trust is necessary for a successful outsourcing relationship, however, the company must be protected by a policy that details and enforces the terms of the outsourcing relationship.

2.0 Purpose

The purpose of this policy is to specify actions to take when selecting a provider of outsourced IT services, standards for secure communications with the provider, and what contractual terms should be in place to protect the company.

3.0 Scope

This policy covers any IT services being considered for outsourcing.

4.0 Policy

4.1 Deciding to Outsource

Outsourcing IT services is often necessary but should be carefully considered, since by nature a certain amount of control will be lost by doing so. The following questions must be affirmatively answered before outsourcing is considered:

- Can the service be performed better or less expensively by a third party provider?
- Would it be cost-prohibitive or otherwise unreasonable to perform this service in-house?
- Will outsourcing the service positively affect the quality of this service?
- Is the cost of this service worth the benefit?
- Are any risks associated with outsourcing the service worth the benefit?

4.2 Outsourcing Core Functions

The company permits the outsourcing of critical and/or core functions of the company's Information Technology infrastructure as long as this policy is followed. Examples of these types of functions are data backups, remote access, security, and network management.

4.3 Evaluating a Provider

Once the decision to outsource an Information Technology function has been made, selecting the appropriate provider is critical to the success of the endeavor. Due diligence must be performed after the potential providers have been pared to a short list of two to three companies. Due diligence must always be performed prior to a provider being selected.

Due diligence should include an evaluation of the provider's ability to perform the requested services, and must specifically cover the following areas:

- Technical ability of the provider
- Ability to deliver the service
- Experience of the provider
- Reputation of the provider
- Policies and procedures related to the service
- Financial strength of the provider
- Service Level Agreements related to the service

If the outsourced service will involve the provider having access to, or storing the company's confidential information, due diligence must cover the provider's security controls for access to the confidential information.

4.4 Security Controls

The outsourcing contract must provide a mechanism for secure information exchange with the service provider. This will vary with the type of service being outsourced, but may include remote access, VPN, or encrypted file exchange.

The company and provider must also maintain a mechanism for verifying the identity of the other party and confirming changes to the service. This will prevent an attacker from using social engineering tactics to gain access to company data.

4.5 Outsourcing Contracts

All outsourced Information Technology services must be governed by a legal contract, with an original of the executed contract maintained by the company.

Contracts must:

- Cover a specified time period
- Specify exact pricing for the services
- Specify how the provider will treat confidential information
- Include a non-disclosure agreement
- Specify services to be provided, including Service Level Agreements and penalties for missing the levels
- Allow for cancellation if contractual terms are not met
- Specify standards for subcontracting of the services and reassignment of contract
- Cover liability issues
- Describe how and where to handle contractual disputes

4.6 Access to Information

The provider must be given the least amount of network, system, and/or data access required to perform the contracted services. This access must follow applicable policies and be periodically audited.

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 Manager and/or executive 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.

6.0 Definitions

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

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.

Network Management A far-reaching term that refers to the process of maintaining and administering a network to ensure its availability, performance, and security.

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.

VPN A secure network implemented over an insecure medium, created by using encrypted tunnels for communication between endpoints.

7.0 Revision History

Revision 1.2 4/30/2008

TruDiligence, LLC

Password Policy	Created: 3/3/2009
Section of: Corporate Security Policies	Target Audience: Users, Technical
CONFIDENTIAL	Page 1 of 4

TruDiligence, LLC is hereinafter referred to as "the company."

1.0 Overview

A solid password policy is perhaps the most important security control an organization can employ. Since the responsibility for choosing good passwords falls on the users, a detailed and easy-to-understand policy is essential.

2.0 Purpose

The purpose of this policy is to specify guidelines for use of passwords. Most importantly, this policy will help users understand why strong passwords are a necessity, and help them create passwords that are both secure and useable. Lastly, this policy will educate users on the secure use of passwords.

3.0 Scope

This policy applies to any person who is provided an account on the organization's network or systems, including: employees, guests, contractors, partners, vendors, etc.

4.0 Policy

4.1 Construction

The best security against a password incident is simple: following a sound password construction strategy. The organization mandates that users adhere to the following guidelines on password construction:

- Passwords should be at least 6 characters

- Passwords should be comprised of a mix of letters, numbers and special characters (punctuation marks and symbols)

- Passwords should be comprised of a mix of upper and lower case characters

- Passwords should not be comprised of, or otherwise utilize, words that can be found in a

dictionary

- Passwords should not be comprised of an obvious keyboard sequence (i.e., qwerty)

- Passwords should not include "guessable" data such as personal information about yourself, your spouse, your pet, your children, birthdays, addresses, phone numbers, locations, etc.

Creating and remembering strong passwords does not have to be difficult. Substituting numbers for letters is a common way to introduce extra characters - a '3' can be used for an 'E,' a '4' can be used for an 'A,' or a '0' for an 'O.' Symbols can be introduced this was as well: an 'S' can become a `,' or an 'i' can be changed to a '!.'

Another way to create an easy-to-remember strong password is to think of a sentence, and then use the first letter of each word as a password. The sentence: 'The quick brown fox jumps over the lazy dog!' easily becomes the password 'Tqbfjotld!'. Of course, users may need to add additional characters and symbols required by the Password Policy, but this technique will help make strong passwords easier for users to remember.

4.2 Confidentiality

Passwords should be considered confidential data and treated with the same discretion as any of the organization's proprietary information. The following guidelines apply to the confidentiality of organization passwords:

- Users must not disclose their passwords to anyone

- Users must not share their passwords with others (co-workers, supervisors, family, etc.)

- Users must not write down their passwords and leave them unsecured

- Users must not check the "save password" box when authenticating to applications

- Users must not use the same password for different systems and/or accounts

- Users must not send passwords via email

- Users must not re-use passwords

4.3 Change Frequency

In order to maintain good security, passwords should be periodically changed. This limits the damage an attacker can do as well as helps to frustrate brute force attempts. At a minimum, users must change passwords every 90 days. The organization may use software that enforces this policy by expiring users' passwords after this time period.

4.4 Applicability of Other Policies

This document is part of the organization'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.

4.5 Incident Reporting

Since compromise of a single password can have a catastrophic impact on network security, it is the user's responsibility to immediately report any suspicious activity involving his or her passwords to the IT Manager. Any request for passwords over the phone or email, whether the request came from organization personnel or not, should be expediently reported. When a password is suspected to have been compromised the IT Manager will request that the user, or users, change all his or her passwords.

5.0 Enforcement

This policy will be enforced by the IT Manager, who may use automated tools to audit and enforce compliance. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment.

6.0 Definitions

Authentication A security method used to verify the identity of a user and authorize access to a system or network.

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

Two Factor Authentication A means of authenticating a user that utilizes two methods: something the user has, and something the user knows. Examples are smart cards, tokens, or

biometrics, in combination with a password.

7.0 Revision History

Revision 1.2 4/30/2008

TruDiligence, LLC

Physical Security Policy	Created: 3/3/2009
Section of: Corporate Security Policies	Target Audience: Technical
CONFIDENTIAL	Page 1 of 8

TruDiligence, LLC is hereinafter referred to as "the company."

1.0 Overview

Information assets are necessarily associated with the physical devices on which they reside. Information is stored on workstations and servers and transmitted on the company's physical network infrastructure. In order to secure the company data, thought must be given to the security of the company's physical Information Technology (IT) resources to ensure that they are protected from standard risks.

2.0 Purpose

The purpose of this policy is to protect the company's physical information systems by setting standards for secure operations.

3.0 Scope

This policy applies to the physical security of the company's information systems, including, but not limited to, all company-owned or company-provided network devices, servers, personal computers, mobile devices, and storage media. Additionally, any person working in or visiting the company's office is covered by this policy.

Please note that this policy covers the physical security of the company's Information Technology infrastructure, and does not cover the security of non-IT items or the important topic of employee security. While there will always be overlap, care must taken to ensure that this policy is consistent with any existing physical security policies.

4.0 Policy

4.1 Choosing a Site

When possible, thought should be given to selecting a site for IT Operations that is secure and free of unnecessary environmental challenges. This is especially true when selecting a datacenter or a site for centralized IT operations. At a minimum, the company's site should meet the following criteria:

- A site should not be particularly susceptible to fire, flood, earthquake, or other natural disasters.

- A site should not be located in an area where the crime rate and/or risk of theft is higher than average.

- A site should have the fewest number of entry points possible.

If these criteria cannot be effectively met for any reason, the company should consider outsourcing its data in whole or in part to a third-party datacenter or hosting provider, provided that such a company can cost effectively meet or exceed the company's requirements.

4.2 Security Zones

At a minimum, the company will maintain standard security controls, such as locks on exterior doors and/or an alarm system, to secure the company's assets. In addition to this the company must provide security in layers by designating different security zones within the building. Security zones should include:

Public This includes areas of the building or office that are intended for public access.

- Access Restrictions: None

- Additional Security Controls: None

- Examples: Lobby, common areas of building

Company This includes areas of the building or office that are used only by employees and other persons for official company business.

- Access Restrictions: Only company personnel and approved/escorted guests

- Additional Security Controls: Additional access controls should be used, such as keys, keypads, keycards, or similar devices, with access to these areas logged if possible.

- Examples: Hallways, private offices, work areas, conference rooms

Private This includes areas that are restricted to use by certain persons within the company, such as executives, scientists, engineers, and IT personnel, for security or safety reasons.

- Access Restrictions: Only specifically approved personnel

- Additional Security Controls: Additional access controls must be used, such as keys, keypads, keycards, or similar devices, with access to these areas logged. Additionally, an alarm system should be considered for these areas that will alert to unauthorized access.

- Examples: Executive offices, lab space, network room, manufacturing area, financial offices, and storage areas.

4.3 Access Controls

Access controls are necessary to restrict entry to the company premises and security zones to only approved persons. There are a several standard ways to do this, which are outlined in this section, along with the company's guidelines for their use.

4.3.1 Keys & Keypads

The use of keys and keypads is acceptable, as long as keys are marked "do not duplicate" and their distribution is limited. These security mechanisms are the most inexpensive and are the most familiar to users. The disadvantage is that the company has no control, aside from changing the locks or codes, over how and when the access is used. Keys can be copied and keypad codes can be shared or seen during input. However, used in conjunction with another security strategy, such as an alarm system, good security can be obtained with keys and keypads.

4.3.2 Keycards & Biometrics

While keycards and biometrics are allowable forms of access controls, the company does not require their use at this time.

Keycards and biometrics have an advantage over keys in that access policies can be tuned to the individual user. Schedules can be set to forbid off-hours access, or forbid users from accessing a security zone where they are not authorized. Perhaps best of all, these methods allow for control over exactly who possesses the credentials. If a keycard is lost or stolen it can be immediately disabled. If an employee is terminated or resigns, that user's access can be disabled. The granular control offered by keycards and biometrics make them appealing access control methods.

4.3.3 Alarm System

A security alarm system is a good way to minimize risk of theft, or reduce loss in the event of a theft. The company mandates the use of professionally monitored alarm

system. The system must be monitored 24x7, with company personnel being notified if an alarm is tripped at any time.

4.4 Physical Data Security

Certain physical precautions must be taken to ensure the integrity of the company's data. At a minimum, the following guidelines must be followed:

- Computer screens should be positioned where information on the screens cannot be seen by outsiders.

- Confidential and sensitive information should not be displayed on a computer screen where the screen can be viewed by those not authorized to view the information.

- Users must log off or shut down their workstations when leaving for an extended time period, or at the end of the workday.

- Network cabling should not run through unsecured areas unless the cabling is carrying only public data (i.e., extended wiring for an Internet circuit).

- The company recommends disabling network ports that are not in use.

4.5 Physical System Security

In addition to protecting the data on the company's information technology assets, this policy provides the guidelines below on keeping the systems themselves secure from damage or theft.

4.5.1 Minimizing Risk of Loss and Theft

In order to minimize the risk of data loss through loss or theft of company property, the following guidelines must be followed:

- Unused systems: If a system is not in use for an extended period of time it should be moved to a secure area or otherwise secured.

- Mobile devices: Special precautions must be taken to prevent loss or theft of mobile devices. Refer to the company's Mobile Device Policy for guidance.

- Systems that store confidential data: Special precautions must be taken to prevent loss or theft of these systems. Refer to the company's Confidential Data Policy for guidance.

4.5.2 Minimizing Risk of Damage

Systems that store company data are often sensitive electronic devices that are susceptible to being inadvertently damaged. In order to minimize the risk of damage, the following guidelines must be followed:

- Environmental controls should keep the operating environment of company systems within standards specified by the manufacturer. These standards often involve, but are not limited to, temperature and humidity.

- Proper grounding procedures must be followed when opening system cases. This may include use of a grounding wrist strap or other means to ensure that the danger from static electricity is minimized.

- Strong magnets must not be used in proximity to company systems or media.

- Except in the case of a fire suppression system, open liquids must not be located above company systems. Technicians working on or near company systems should never use the systems as tables for beverages. Beverages must never be placed where they can be spilled onto company systems.

- Uninterruptible Power Supplies (UPSs) and/or surge-protectors are required for important systems and encouraged for all systems. These devices must carry a warranty that covers the value of the systems if the systems were to be damaged by a power surge.

4.6 Fire Prevention

It is the company's policy to provide a safe workplace that minimizes the risk of fire. In addition to the danger to employees, even a small fire can be catastrophic to computer systems. Further, due to the electrical components of IT systems, the fire danger in these areas is typically higher than other areas of the company's office. The guidelines below are intended to be specific to the company's information technology assets and should conform to the company's overall fire safety policy.

- Fire, smoke alarms, and/or suppression systems must be used, and must conform to local fire codes and applicable ordinances.

- Electrical outlets must not be overloaded. Users must not chain multiple power strips, extension cords, or surge protectors together.

• Extension cords, surge protectors, power strips, and uninterruptible power supplies must be of the three-wire/three-prong variety.

• Unused electrical equipment should be turned off when not in use for extended periods of time (i.e., during non-business hours) if practical.

• Periodic inspection of electrical equipment must be performed. Power cords, cabling, and other electrical devices must be checked for excessive wear or cracks. If overly-worn equipment is found, the equipment must be replaced or taken out of service immediately depending on the degree of wear.

• A smoke alarm monitoring service should be considered that will alert a designated company employee if an alarm is tripped during non-business hours.

4.7 Entry Security

It is the company's policy to provide a safe workplace for employees. Monitoring those who enter and exit the premises is a good security practice in general, but is particularly true for minimizing risk to company systems and data. The guidelines below are intended to be specific to the company's information technology assets and should conform to the company's overall security policy.

4.7.1 Use of Identification Badges

Identification (ID) badges are useful to identify authorized persons on the company premises. The company has established the following guidelines for the use of ID badges.

• Employees: ID badges are not required.

• Non-employees/Visitors: Visitor badges are not required, though generic visitor badges are encouraged.

4.7.2 Sign-in Requirements

The company does not wish to establish any requirements for employee/visitor sign-in. Use of a visitor sign-in register is encouraged.

4.7.3 Visitor Access

Visitors should be given only the level of access to the company premises that is appropriate to the reason for their visit. After checking in, visitors must be escorted

unless they are considered "trusted" by the company. Examples of a trusted visitor may be the company's legal counsel, financial advisor, or a courier that frequents the office, and will be decided on a case-by-case basis.

4.8 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 Manager and/or executive 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.

6.0 Definitions

Biometrics The process of using a person's unique physical characteristics to prove that person's identity. Commonly used are fingerprints, retinal patterns, and hand geometry.

Datacenter A location used to house a company's servers or other information technology assets. Typically offers enhanced security, redundancy, and environmental controls.

Keycard A plastic card that is swiped, or that contains a proximity device, that is used for identification purposes. Often used to grant and/or track physical access.

Keypad A small keyboard or number entry device that allows a user to input a code for authentication purposes. Often used to grant and/or track physical access.

Mobile Device A portable device that can be used for certain applications and data storage. Examples are PDAs or Smartphones.

PDA Stands for Personal Digital Assistant. A portable device that stores and organizes personal information, such as contact information, calendar, and notes.

Smartphone A mobile telephone that offers additional applications, such as PDA functions and email.

Uninterruptible Power Supplies (UPSs) A battery system that automatically provides power to electrical devices during a power outage for a certain period of time. Typically also contains power surge protection.

7.0 Revision History

Revision 1.2 4/30/2008

TruDiligence, LLC

Remote Access Policy	Created: 3/3/2009
Section of: Corporate Security Policies	Target Audience: Users, Technical
CONFIDENTIAL	Page 1 of 3

TruDiligence, LLC is hereinafter referred to as "the company."

1.0 Overview

It is often necessary to provide access to corporate information resources to employees or others working outside the company's network. While this can lead to productivity improvements it can also create certain vulnerabilities if not implemented properly. The goal of this policy is to provide the framework for secure remote access implementation.

2.0 Purpose

This policy is provided to define standards for accessing corporate information technology resources from outside the network. This includes access for any reason from the employee's home, remote working locations, while traveling, etc. The purpose is to define how to protect information assets when using an insecure transmission medium.

3.0 Scope

The scope of this policy covers all employees, contractors, and external parties that access company resources over a third-party network, whether such access is performed with company-provided or non-company-provided equipment.

4.0 Policy

4.1 Prohibited Actions

Remote access to corporate systems is only to be offered through a company-provided means of remote access in a secure fashion. The following are specifically prohibited:

- Installing a modem, router, or other remote access device on a company system without the approval of the IT Manager.

- Remotely accessing corporate systems with a remote desktop tool, such as VNC, Citrix, or GoToMyPC without the written approval from the IT Manager.

- Use of non-company-provided remote access software.

- Split Tunneling to connect to an insecure network in addition to the corporate network, or in order to bypass security restrictions.

4.2 Use of non-company-provided Machines

Accessing the corporate network through home or public machines can present a security risk, as the company cannot completely control the security of the system accessing the network. Use of non-company-provided machines to access the corporate network is permitted as long as this policy is adhered to, and as long as the machine meets the following criteria:

- It has up-to-date antivirus software installed
- Its software patch levels are current
- It is protected by a firewall

When accessing the network remotely, users must not store confidential information on home or public machines.

4.3 Client Software

The company will supply users with remote access software that allows for secure access and enforces the remote access policy. The software will provide traffic encryption in order to protect the data during transmission as well as a firewall that protects the machine from unauthorized access.

4.4 Network Access

There are no restrictions on what information or network segments users can access when working remotely, however the level of access should not exceed the access a user receives when working in the office.

4.5 Idle Connections

Due to the security risks associated with remote network access, it is a good practice to dictate that idle connections be timed out periodically. Remote connections to the company's network must be timed out after 1 hour of inactivity.

4.6 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 Manager and/or executive 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.

6.0 Definitions

Modem A hardware device that allows a computer to send and receive digital information over a telephone line.

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.

Split Tunneling A method of accessing a local network and a public network, such as the Internet, using the same connection.

Timeout A technique that drops or closes a connection after a certain period of inactivity.

Two Factor Authentication A means of authenticating a user that utilizes two methods: something the user has, and something the user knows. Examples are smart cards, tokens, or biometrics, in combination with a password.

7.0 Revision History

Revision 1.2 4/30/2008

TruDiligence, LLC

Retention Policy	Created: 3/3/2009
Section of: Corporate Security Policies	Target Audience: Users, Technical
CONFIDENTIAL	Page 1 of 4

TruDiligence, LLC is hereinafter referred to as "the company."

1.0 Overview

The need to retain data varies widely with the type of data. Some data can be immediately deleted and some must be retained until reasonable potential for future need no longer exists. Since this can be somewhat subjective, a retention policy is important to ensure that the company's guidelines on retention are consistently applied throughout the organization.

2.0 Purpose

The purpose of this policy is to specify the company's guidelines for retaining different types of data.

3.0 Scope

The scope of this policy covers all company data stored on company-owned, company-leased, and otherwise company-provided systems and media, regardless of location.

Note that the need to retain certain information can be mandated by local, industry, or federal regulations. Where this policy differs from applicable regulations, the policy specified in the regulations will apply.

4.0 Policy

4.1 Reasons for Data Retention

The company does not wish to simply adopt a "save everything" mentality. That is not practical or cost-effective, and would place an excessive burden on the IT Staff to manage the constantly-growing amount of data.

Some data, however, must be retained in order to protect the company's interests, preserve evidence, and generally conform to good business practices. Some reasons for data retention include:

- Litigation

- Accident investigation
- Security incident investigation
- Regulatory requirements
- Intellectual property preservation

4.2 Data Duplication

As data storage increases in size and decreases in cost, companies often err on the side of storing data in several places on the network. A common example of this is where a single file may be stored on a local user's machine, on a central file server, and again on a backup system. When identifying and classifying the company's data, it is important to also understand where that data may be stored, particularly as duplicate copies, so that this policy may be applied to all duplicates of the information.

4.3 Retention Requirements

This section sets guidelines for retaining the different types of company data.

Personal There are no retention requirements for personal data. In fact, the company requires that it be deleted or destroyed when it is no longer needed.

Public Public data must be retained for 3 years.

Operational Most company data will fall in this category. Operational data must be retained for 5 years.

Critical Critical data must be retained for 7 years.

Confidential Confidential data must be retained for 7 years.

4.4 Retention of Encrypted Data

If any information retained under this policy is stored in an encrypted format, considerations must be taken for secure storage of the encryption keys. Encryption keys must be retained as long as the data that the keys decrypt is retained.

4.5 Data Destruction

Data destruction is a critical component of a data retention policy. Data destruction ensures that the company will not get buried in data, making data management and data retrieval more complicated and expensive than it needs to be. Exactly how certain data should be destroyed is covered in the Data Classification Policy.

When the retention timeframe expires, the company must actively destroy the data covered by this policy. If a user feels that certain data should not be destroyed, he or she should identify the data to his or her supervisor so that an exception to the policy can be considered. Since this decision has long-term legal implications, exceptions will be approved only by a member or members of the company's executive team.

The company specifically directs users not to destroy data in violation of this policy. Particularly forbidden is destroying data that a user may feel is harmful to himself or herself, or destroying data in an attempt to cover up a violation of law or company policy.

4.6 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 Manager and/or executive 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 are suspected, the company will 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.

Encryption The process of encoding data with an algorithm so that it is unintelligible and secure 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.

7.0 Revision History

Revision 1.3 4/30/2008

TruDiligence, LLC

Third Party Connection Policy	Created: 3/3/2009
Section of: Corporate Security Policies	Target Audience: Technical
CONFIDENTIAL	Page 1 of 3

TruDiligence, LLC is hereinafter referred to as "the company."

1.0 Overview

Direct connections to external entities are sometimes required for business operations. These connections are typically to provide access to vendors or customers for service delivery. Since the company's security policies and controls do not extend to the users of the third parties' networks, these connections can present a significant risk to the network and thus require careful consideration.

2.0 Purpose

The policy is intended to provide guidelines for deploying and securing direct connections to third parties.

3.0 Scope

The scope of this policy covers all direct connections to the company's network from non-company owned networks. This policy excludes remote access and Virtual Private Network (VPN) access, which are covered in separate policies.

4.0 Policy

4.1 Use of Third Party Connections

Third party connections are to be discouraged and used only if no other reasonable option is available. When it is necessary to grant access to a third party, the access must be restricted and carefully controlled. A requester of a third party connection must demonstrate a compelling business need for the connection. This request must be approved and implemented by the IT Manager.

4.2 Security of Third Party Access

Third party connections require additional scrutiny. The following statements will govern these connections:

- Connections to third parties must use a firewall or Access Control List (ACL) to separate

the company's network from the third party's network.

- Third parties will be provided only the minimum access necessary to perform the function requiring access. If possible this should include time-of-day restrictions to limit access to only the hours when such access is required.

- Wherever possible, systems requiring third party access should be placed in a public network segment or demilitarized zone (DMZ) in order to protect internal network resources.

- If a third party connection is deemed to be a serious security risk, the IT Manager will have the authority to prohibit the connection. If the connection is absolutely required for business functions, additional security measures should be taken at the discretion of the IT Manager.

4.3 Restricting Third Party Access

Best practices for a third party connection require that the link be held to higher security standards than an intra-company connection. As such, the third party must agree to:

- Restrict access to the company's network to only those users that have a legitimate business need for access.

- Provide the company with the names and any other requested information about individuals that will have access to the connection. The company reserves the right to approve or deny this access based on its risk assessment of the connection.

- Supply the company with on-hours and off-hours contact information for the person or persons responsible for the connection.

- (If confidential data is involved) Provide the company with the names and any other requested information about individuals that will have access to the company's confidential data. The steward or owner of the confidential data will have the right to approve or deny this access for any reason.

4.4 Auditing of Connections

In order to ensure that third-party connections are in compliance with this policy, they must be audited periodically.

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 Manager and/or executive 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.

6.0 Definitions

Access Control List (ACL) A list that defines the permissions for use of, and restricts access to, network resources. This is typically done by port and IP address.

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.

Firewall A security system that secures the network by enforcing boundaries between secure and insecure areas. Firewalls are often implemented at the network perimeter as well as in high-security or high-risk areas.

Third Party Connection A direct connection to a party external to the company. Examples of third party connections include connections to customers, vendors, partners, or suppliers.

7.0 Revision History

Revision 1.2 4/30/2008

TruDiligence, LLC

VPN Policy	Created: 3/3/2009
Section of: Corporate Security Policies	Target Audience: Technical
CONFIDENTIAL	Page 1 of 3

TruDiligence, LLC 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 Manager.

4.5 Logging and Monitoring

Depending on the nature of the site-to-site VPN, the IT Manager 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 yearly.

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 Manager and/or executive 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.

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 1.2 4/30/2008

TruDiligence, LLC

Wireless Access Policy	Created: 3/3/2009
Section of: Corporate Security Policies	Target Audience: Technical
CONFIDENTIAL	Page 1 of 4

TruDiligence, LLC is hereinafter referred to as "the company."

1.0 Overview

Wireless communication is playing an increasingly important role in the workplace. In the past, wireless access was the exception; it has now become the norm in many companies. However, while wireless access can increase mobility and productivity of users, it can also introduce security risks to the network. These risks can be mitigated with a sound Wireless Access Policy.

2.0 Purpose

The purpose of this policy is to state the standards for wireless access to the company's network. Wireless access can be done securely if certain steps are taken to mitigate known risks. This policy outlines the steps the company wishes to take to secure its wireless infrastructure.

3.0 Scope

This policy covers anyone who accesses the network via a wireless connection. The policy further covers the wireless infrastructure of the network, including access points, routers, wireless network interface cards, and anything else capable of transmitting or receiving a wireless signal.

4.0 Policy

4.1 Physical Guidelines

Unless a directional antenna is used, a wireless access point typically broadcasts its signal in all directions. For this reason, access points must be located central to the office space rather than along exterior walls. Technology must be used to control the signal broadcast strength so that it is reduced to only what is necessary to cover the office space. Directional antennas must be used as necessary to focus the signal to areas where it is needed.

Physical security of access points must be considered. Access points must be placed in secured areas of the office. Cabling to and from access points should be secured so that it cannot be accessed without difficulty.

4.2 Configuration and Installation

The following guidelines apply to the configuration and installation of wireless networks:

4.2.1 Security Configuration

- The Service Set Identifier (SSID) of the access point must be changed from the factory default. The SSID must be changed to something completely nondescript. Specifically, the SSID must not identify the company, the location of the access point, or anything else that may allow a third party to associate the access point's signal to the company.

- The SSID must not be broadcast. This adds a layer of security by requiring wireless users to know the SSID in order to connect to the network.

- The wireless access point must utilize Mac address filtering so that only known wireless NICs are able to connect to the wireless network.

- The wireless access point must not connect to the company's trusted network without a firewall or other form of access control separating the two networks.

- Encryption must be used to secure wireless communications. The strongest available algorithm must be used (i.e., WPA rather than WEP). Encryption keys must be changed and redistributed quarterly.

- Administrative access to wireless access points must utilize strong passwords.

- All logging features must be enabled on the company's access points.

- Wireless networking should require users to authenticate against a centralized server. These connections should be logged, with IT staff reviewing the log regularly for unusual or unauthorized connections.

- Wireless LAN management software should be used to enforce wireless security policies. The software must have the capability to detect rogue access points.

- Users accessing the wireless network must be provided a personal software

firewall to secure their computers.

4.2.2 Installation

- Software and/or firmware on the wireless access points and wireless network interface cards (NICs) must be updated prior to deployment.

- Wireless networking must not be deployed in a manner that will circumvent the company's security controls.

- Wireless devices must be installed only by the company's IT department.

- Channels used by wireless devices must be evaluated to ensure that they do not interfere with company equipment.

4.3 Accessing Confidential Data

Wireless access to confidential data is permitted as long as the access is consistent with this and other policies that apply to confidential data.

4.4 Inactivity

Users must disable their wireless capability when not using the wireless network. This will reduce the chances that their machine could be compromised from the wireless NIC.

Inactive wireless access points must be disabled. If not regularly used and maintained, inactive access points represent an unacceptable risk to the company.

Wireless access points must be disabled during non-business hours. This should be accomplished with management software rather than manually performed.

4.5 Audits

The wireless network must be audited quarterly to ensure that this policy is being followed. Specific audit points should be: location of access points, signal strength, SSID, SSID broadcast, and use of strong encryption.

4.6 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 Manager and/or executive 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.

6.0 Definitions

Mac Address Short for Media Access Control Address. The unique hardware address of a network interface card (wireless or wired). Used for identification purposes when connecting to a computer network.

SSID Stands for Service Set Identifier. The name that uniquely identifies a wireless network.

WEP Stands for Wired Equivalency Privacy. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. WEP can be cryptographically broken with relative ease.

WiFi Short for Wireless Fidelity. Refers to networking protocols that are broadcast wirelessly using the 802.11 family of standards.

Wireless Access Point A central device that broadcasts a wireless signal and allows for user connections. A wireless access point typically connects to a wired network.

Wireless NIC A Network Interface Card (NIC) that connects to wireless, rather than wired, networks.

WPA Stands for WiFi Protected Access. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. Newer and considered more secure than WEP.

7.0 Revision History

Revision 1.2 4/30/2008