



INFORMATION SECURITY POLICY

Contents

- Policy Statement..... 2**
 - Reason for Policy/Purpose..... 2
 - Who Needs to Know This Policy 2
- Policy/Procedures 3**
 - A. Physical Security of IT Computing Resources 3
 - B. Passwords 3
 - C. Securing Your PC..... 4
 - D. Confidentiality 4
 - E. Availability..... 5
 - F. Integrity..... 5
- Website Addresses for This Policy 6**
- Contacts..... 6**
- Related Information..... 6**
- Who Approved This Policy 7**
- History/Revision Dates..... 7**
- Appendices 8**
 - Appendix A..... 8
 - Passwords, Personal Identification Numbers (PINs), and Other Login Controls..... 8
 - Appendix B 10
 - Reporting a Security Related Incident 10
 - Appendix C..... 13
 - Detailed Roles and Responsibilities Guidance for All Users 13

Policy Statement

Maintaining the integrity of information stored in eDiscovery Tools systems is a responsibility shared by all users of those systems. All Information Technology (IT) computing resource users are responsible for protecting company information, and are expected to be familiar with and comply with this policy. Violations of this policy may result in disciplinary action up to and including dismissal.

Reason for Policy/Purpose

Information is a vital company asset and requires protection from unauthorised access, modification, disclosure or destruction. This policy sets forth requirements and guidelines for incorporation of information security practices into daily usage of company IT computing resources.

Who Needs to Know This Policy

Staff and clients.

Policy/Procedures

Users of company IT computing resources are responsible for protecting the information processed, stored, or transmitted over or on those resources, and for incorporating the following practices into their daily usage of such resources.

A. Physical Security of IT Computing Resources

Company technology assets require physical security measures to protect theft and loss of information. Further, if a computer is stolen it can take hundreds or even thousands of hours to re-create the information lost with the hardware. Users of IT resources should:

1. Always use a security cable or locking device with laptop computers;
2. Lock office doors when leaving;
3. Never remove asset tags from equipment;
4. Lock away laptops, PDAs or computer peripherals overnight in accordance with the Laptop Computer and Small Electronic Device Theft Policy;
5. Configure a password-protected screen saver;
6. Logout of the system when finished working; and
7. Utilise a power-on password.

B. Passwords

Passwords are an integral part of overall security. To minimize the risk of a password being compromised and data being lost due to unauthorised access, employ the following:

1. Do not use familiar names;
2. Avoid using commonly known facts about yourself;
3. Do not use words found in the dictionary;
4. Use at least eight (8) characters;
5. Utilise both letters and numbers;
6. Use special characters if possible;

7. Use upper-case and lower-case letters if possible;
8. Combine misspelled words;
9. Do not share your password with anyone;
10. Never write down your password in an area where it can be linked to your specific computer or account;
11. Do not store your password in a computer file;
12. When receiving technical assistance, enter your password instead of telling it to the technology staff member; and
13. If you ever receive a telephone call from someone claiming to need your password, report it immediately.

For more password “Do’s and Don’ts,” or to check the strength of a sample password, see Appendix A: Passwords, Personal Identification Numbers (PINs), and Other Login Controls.

C. Securing Your PC

It is important to maintain company computers up-to-date with the latest electronic security measures to prevent viruses and worms from spreading from one machine to another, and to minimize the opportunity for hackers to damage or steal data. Accordingly, IT computing resource users should employ the following:

1. Keep anti-virus software up to date. A free 30 day copy of NOD 32 can be found at <http://eset.com.au/>
2. Keep systems patched
3. Use a personal firewall (recommended)

See Securing Your Workstation for further information and guidance.

D. Confidentiality

All members of the company are obligated to respect and in many cases to protect confidential data, and to follow the Data Classification Security Policy. The company strongly discourages storage of any confidential or sensitive data on any computer or network-attached device that has not been explicitly approved by company information security personnel. As such, IT computing resource users shall adhere to the following:

1. Employ adequate encryption technology for sensitive or critical information such as identification numbers and credit card numbers. For specific information regarding encryption technology options, e-mail support@ediscoverytools.com.

2. Notify the Chief Security Officer at support@ediscoverytools.com if sensitive or critical company information is lost or disclosed to unauthorised parties, if any unauthorized use of company systems has taken place, or if there is suspicion of such loss, disclosure or unauthorised use.
3. DO NOT post company material such as software, internal memos, or other non-public information on any publicly-accessible computer unless first approved by the appropriate authority.
4. DO NOT place company sensitive or critical information in any computer unless the persons who have access to that computer have a legitimate need-to-know the information involved.
5. DO NOT save fixed passwords in web browsers or e-mail clients when using a company system. This may allow unauthorized users to access critical or sensitive information such that contained in Banner or the Enterprise Accounting System.
6. DO NOT distribute internal critical or sensitive company communications to external entities that are not affiliated with the company. Only distribute to internal entities on a need to know basis.
7. DO NOT establish Internet or other external network connections that could allow non-company users to gain access to company systems with critical or sensitive information unless prior approval has been received by the appropriate authority.
8. DO NOT discuss information security-related incidents with individuals outside of the company, or with those inside the company who do not have a need-to-know.

E. Availability

Company systems and IT computing resources are expected to be available and ready for usage. Accordingly, resource users are expected to limit usage of these resources to reasonable levels and should assist in making resources available as follows:

1. Update system patches for IT computing resources that transmit, process or store critical or sensitive information.
2. DO NOT probe security mechanisms at either the company or other sites unless authorised to do so by the Senior Software Engineer.
3. DO NOT cause intentional harm to company-owned IT computing resources. This includes intentionally down loading from any source.

F. Integrity

Integrity means ensuring the soundness or completeness of information during its transmission, storage, generation, and/or handling. Information that is modified may be erroneous and could lead to

poor business decisions. In order to maximize integrity, IT computing resource users shall adhere to the following:

1. Screen all non-text files downloaded from the Internet with anti-virus software prior to usage to minimize the risk of corruption, modification or loss of data.
2. Notify the Chief Security Office immediately if passwords or other system access control mechanisms are lost, stolen or disclosed, or are suspected of being lost, stolen or disclosed.
3. Forward information pertaining to security-related problems to the Chief Security Officer immediately. DO NOT personally redistribute system vulnerability information.
4. Review information obtained from the Internet with caution. Before using free Internet-supplied information for business decision-making purposes, corroborate and confirm the information by consulting other reliable sources.
5. Secure personal computers via a locking feature such as a password-protected screen saver when walking away. Public computers with no critical or sensitive information, such as those in the library or in labs, are excluded.

For further information on reporting security incidents, see Appendix B, Reporting a Security Related Incident. For further information on security practices and guidance, see Appendix C, Detailed Roles and Responsibilities Guidance for All Users.

Website Addresses for This Policy

www.ediscoverytools.com/legal.html

Contacts

Chief Security Officer

Subject: Information Security

Contact Email: support@ediscoverytools.com

Related Information

Code of Conduct for Users of Computing Systems and Services

Data Classification Security Policy

Laptop Computer and Small Electronics Theft Policy

Mobile Device Security Policy

Who Approved This Policy

Jo Sherman, Founder and CEO, eDiscovery Tools

History/Revision Dates

Origination Date: September 13, 2006

Last Amended Date: March 16, 2010

Appendices

Appendix A

Passwords, Personal Identification Numbers (PINs), and Other Login Controls

Passwords

For most applications, the company enforces a maximum password “lifetime” of one year, after which the password must be changed. System administrators may set the maximum password lifetime to less than one year for critical or sensitive applications.

Personal Identification Numbers (PINs)

PINs are used for access to web-based applications. Individuals’ data access through web-based applications is typically restricted to data pertaining only to the particular user (e.g., an employee’s own benefit information), and therefore carries lower risk than access to other enterprise applications. Therefore, PINs may have longer lifetimes than application passwords. However, web-based application users are encouraged to use hard-to-guess PINs and change them regularly.

Authorised security administrators, help desk staff, and automated authentication processes reset passwords and PINs, in response to user request and only after receipt of proof of the user’s identity and company affiliation.

Inactivity timeout thresholds—which, when exceeded, trigger termination of the login session—are set for most enterprise business applications.

Access

Access guidelines define access rights and privileges and protect assets and data from loss or inappropriate disclosure by specifying acceptable use guidelines for users, operations staff and management. Access to company enterprise business applications is permitted on the condition that the user observes the Code of Conduct for Users of Computing Systems and Services. Access may be revoked if either the Code of Conduct or this policy is violated; other actions up to and including termination of company employment may also be taken, depending on the particular violation.

- When a user is initially granted an account for a company enterprise business application, access rights are based on legitimate need to access/change data.

- Enterprise business data categories have “owners” (stewards) who are ultimately responsible for the integrity of the data. An application security administrator grants access to specific company Data only after such access is approved by the appropriate data owner.
- For employees and contractors, department managers with knowledge of the individuals’ legitimate need to view and change data initiate requests for access to an application as well as requests to change access. Department managers have responsibility for monitoring their employees’ job responsibilities and access rights to ensure appropriate access levels.
- When a user’s relationship with the company changes, or specific duties change (if an employee or contractor), access rights should be changed to reflect the new relationship/responsibilities.
- The termination of a relationship with the company (e.g., resignation) results in termination of the user’s access rights.
- The company restricts ability to perform changes to security access levels in a production instance of an application to the application’s Security Administrator(s).

Appendix B

Reporting a Security Related Incident

The Chief Security Officer should be contacted via e-mail i.e. support@ediscoverytools.com or via telephone. When contacting the Chief Security Officer, please include the following information if possible:

- The incident time and date
- The incident category
- Information pertaining to how was the incident was discovered
- Business processes affected by the incident
- System(s) affected by the incident including trusted relationships
- Subnets or other IT computing resources affected by the incident
- The physical address where incident occurred
- Witness statement of incident information
- System program information that detected incident
- Operating System version including patch information
- Application version information
- System and Event Logs
- Security protection tools currently used by the affected system(s)
- If applicable, a vulnerability and port scan report of the affected system(s)

Proper Evidence Handling and Chain of Custody

Evidence must be relevant, material, and competent for admissibility in a court of law. Evidence must be collected and preserved based on the Rules of Evidence. Evidence must not be altered. After an incident occurs that impacts a critical system, the machine must be unplugged from the network, and left undisturbed until the Incident Response team leader or other designee advises that it is safe to repair the machine and reconnect the machine to the network. The Information Security Office should be immediately contacted after the discovery of an incident.

Reporting, Escalation, and Tracking

The Chief Security Officer shall provide a high-level status report to Senior Management and the affected business unit manager advising of the computer or information security related incident. The Incident Response Team Leader shall provide a detailed level report laying out the specific details of the incident(s) to the Chief Security Officer regarding incident status. The Incident Response Team Leader shall provide the Incident Response Team with the specifics of the incident(s).

Legal/Public Relation Considerations

Oftentimes there are legal and public relations concerns to consider. In order to take these into account IT computing resource users:

- Shall not perform activities over the Internet that are considered libellous or that defame the character of another person or entity;
- Shall not speak to or communicate publicly with news reporters or similar entities on behalf of the company unless authorized;
- Shall not misrepresent, obscure, suppress, or replace a user's identity on the Internet or any company electronic communications system;
- Shall not make threats against another user or organization over the Internet;
- Shall not use the Internet to harass, annoy, or alarm another person; and
- Shall not use the Internet as a means to facilitate criminal or other illegal activity.
- Shall not violate the intellectual property rights of any owner of intellectual property.

Security and Technical Support Roles and Responsibilities

Roles and Responsibilities

Managers

- Are required to provide technical support staff with the appropriate qualifications for provision of technical support to all staff and resources.
- Are required to clearly identify what will be supported by the technical support staff. Security Awareness Training is available so that current security requirements are understood.
- Are required to provide system administration staff with the appropriate resources to maintain and secure department owner servers.
- Are required to provide for the professional development of technical support staff and system administration staff so that staff skills are up to date.
- Are required to provide for IT computing resources and maintenance cost associated with the IT computing resource.

Roles and Responsibilities

Information Systems and Services

- Is required to provide a check list of qualifications required for all technical support staff and system administrators.
- Is required to assist in the selection of qualified technical support staff and system administrators if requested by deans or department heads.
- Is required to clearly identify what will be supported by ISS to enable managers to determine gaps in support.
- Is required to offer assistance to technical support and system administration staff in troubleshooting complex problems.
- Is required to provide system administration and security guidelines for system administrators of department servers to follow.
- Is required to sustain The Information Security Office.
 - The Information Security Office is required to create, develop and communicate company-wide computer security policies and programs that support the confidentiality, integrity, and availability of systems owned by the company.
 - The Information Security Office investigates and has the authoritative oversight relating to system intrusions and other information security incidents.
 - The Information Security Office provides guidance and direction regarding information security related activities.

*Roles and Responsibilities**Local Support Partners*

- Are required to support all core software applications of the company, as well as the minimum support hardware configurations for the business unit in which they support.
- Are required to maintain desktop information security for all systems in their department. At a minimum, this includes distributing and updating anti-virus software and keeping operating systems updated and patched.
- Are required to log and track all support calls
- Will report security violations to the Information Security Office and act as the contact point for security assessments and monitoring efforts.

*Roles and Responsibilities**Staff*

- Take reasonable steps to secure desktop and server systems under the control of such staff. Contact the LSP for additional information and options.
- Not store sensitive information on systems without coordination and approval by ISS Security / appropriate data owner. Sensitive information includes, but is not limited to identity numbers, credit card numbers and protected information covered under legislation such as FERPA, GLB, and HIPAA.
- Report security incidents or issues to LSP.
- Comply with code of conduct.
- Update operating system and software patches on their desktop computers regularly.
- Update and install anti-virus software. Systems should be scanned weekly.
- Install personal firewall on desktop computers (recommended).
- Report any security issues to ISS Helpdesk.
- Comply with code of conduct.

Appendix C

Detailed Roles and Responsibilities Guidance for All Users

Everybody handles information in one-way or another. It is important that we all take steps to help secure it. All users of company computing resources are responsible for helping in the protection and proper use of our information and technology resources. The following guidance will assist in that responsibility.

Back-ups

The frequency of backups should depend on the importance of the information, how often it is modified and the impact that its loss would have to our organization.

- Perform a FULL backup whenever possible.
- Do not backup over your most recent backup media.
- Use a cycle of at least three backups to avoid losing data if a tape or other backup media goes bad.
- Frequency of backups should be appropriate for the importance of the data on your computer.
- Properly label your backups to ensure correct rotation and identification.
- Store backup media in a safe and secure location.
- Password protect your backups, if possible.

Document Security

One of the most overlooked areas of security often involves physical documents. These are also information resources and require the same level of protection as their electronic counterparts. Follow these guidelines to make sure your files are where you need them, when you need them:

- Maintain a "clean desk" and keep your work space secured; i.e., lock up any sensitive files and diskettes.
- Don't leave documents unattended on the copier or fax machine.
- Shred any confidential documents when you are discarding them.
- Remove papers and wipe boards clean when finished using conference rooms.
- Lock filing cabinets when you leave.

Hoaxes and Chain Letters

E-mail chain letters and hoaxes ask the receiver to forward the message on to a specified number of people, or as many as possible. However, if you forward a message to just ten people and they each do

the same, and this cycle continues ten times, this would result in 10,000,000,000 (that's 10 billion) messages. If that sounds unbelievable, check for yourself - the calculation is 10 to the 10th power.

You can easily see how this can become a burden on e-mail systems in both traffic and storage capacity.

What makes this even worse is that most e-mail chain letters are based on falsehoods or urban legends. They may reference some reputable source but do not provide any contact information for verification.

- Learn how to recognize hoaxes and chain letters
- Discourage others from forwarding them
- If you're not sure it's a hoax, report it
- Report persistent senders of inappropriate email
- Delete any hoaxes or chain letters you receive
- Don't distribute distasteful jokes or images

Identity Theft

Believe it or not, your personal information can be targeted by thieves. Once obtained, they can use your identity to obtain cash or purchase items using your credit. The results can be a financial nightmare. Take steps to protect yourself by following these tips:

- Never give out financial information to unknown callers
- Guard your credit cards, ATM card, its PIN and receipts
- Immediately report lost or stolen checks and credit cards
- Always shred unwanted financial solicitations
- Store both new and cancelled cheques in a secure location
- Thoroughly review your bills, bank statements and credit card statements; report unauthorized activity
- Consider using a postal service collection box to mail financially-related items instead of using your residential mailbox
- Periodically obtain and review your credit reports

If you believe another member of the company has fraudulently used your information to obtain/use credit, you need to file a police report with the company Police Department so an official case can be opened and addressed.

To best protect against becoming an ID theft victim:

- Be careful about giving out your personal information. For example, don't give out personal identifying information (date of birth, mother's maiden name) to someone over the phone (or the Internet) when you haven't initiated the transaction.
- Put passwords (NOT your mother's maiden name) on credit card and bank accounts, to make it harder for an ID thief to make changes to, or "takeover," your account.
- Order your credit reports once a year from each of the three national credit bureaus. That way you're likely to catch any identity theft before it gets out of hand -- and not when you're waiting for a mortgage application to be approved.

If you discover that your identity has been stolen:

- Call the fraud departments of all three credit bureaus. Ask them to put a "fraud alert" on your file (this tells creditors to call you before they open any more accounts in your name). Also, ask for a copy of your credit report, and ask the credit bureau to remove any fraudulent or incorrect information.
- Contact the credit grantors involved - e.g., the bank or credit card issuers who opened the fraudulent account or permitted access to your existing account.
- Immediately close all affected accounts.
- Contact your local police, and ask to file a report. Even if the police can't catch the identity thief, having a police report can help you in clearing up your credit records later on.

Passwords

Passwords are an integral part of overall security. Unfortunately, they are one of the vulnerabilities most frequently targeted by someone trying to break into a system. If your password is compromised, then anything your user account is able to access could be at risk. There are numerous ways that you can help protect your password and our information.

- Do not use familiar names
- Avoid using commonly known facts about yourself
- Do not use words found in the dictionary
- Use at least eight (8) characters
- Utilize both letters and numbers
- Use special characters, if possible
- Use upper- and lower-case letters, if possible
- Combine misspelled words
- Do not share your password with anyone
- Never write down your password
- Do not store your password in a computer file
- When receiving technical assistance, enter your password instead of telling it to the technology staff member
- If you ever receive a telephone call from someone claiming to need your password, report it immediately

For more password Do's and Don'ts or to check the strength of a sample password go to the following website: <http://infosec.gwu.edu/Program/PWTest.asp>

PC and Laptop Security

The physical security of our technology assets is a serious issue. If a computer is stolen, there is a lot more at stake than just a piece of hardware. It can take hundreds or even thousands of hours to re-create the information that would be missing along with the computer. There are several things that can be done to help reduce the chance of computer theft.

- Always use a security cable or locking device
- Lock your office door when you leave
- Never remove any assets tags from our equipment
- Lock away any laptops, PDAs or computer peripherals overnight
- Configure a password-protected screen saver

- Logout of the system when you are finished working
- Utilize a power-on password

Physical Security

There are things to be aware of to help prevent a mishap that could lead to a loss of our information, personal property, or worse. The key is knowing how to prevent a situation from happening. Consider these words of advice:

- If you expect to be working late, park in an area that will have adequate lighting when you leave.
- When entering secured areas do not let strangers "tailgate" in behind you.
- Never prop open doors that lead to secured areas.
- If you encounter strangers or unknown visitors in secured work areas, ask them if you could be of some assistance with a simple "May I help you?"
- If you ever lose an access card or key, report it immediately to the appropriate person.
- When leaving at night, try to exit with other co-workers if possible. There is some truth to the saying "safety in numbers."

Securing your PC

It is important to maintain your computer up-to-date with the latest patches, fixes, service packs and virus definitions (of your anti-virus software). This prevents computer viruses and worms from spreading from your computer and denies hackers the potential opportunity to damage or steal data from your computer.

- Keep anti-virus software up to date. A free 30 day copy of NOD 32 can be found at <http://eset.com.au/>
- Keep systems patched.
- Use a personal firewall (recommended).

Social Engineering

A social engineer is a person that will deceive or con others into divulging information that they wouldn't normally share. It is one of the most commonly used methods of hacking. By building trust with their victims through deception and lies, a social engineer will try to get information that can be used later -- usually for wrongdoing.

If someone phones or appears and asks you for information that you know is confidential company, client or personal information, don't be afraid to ask them a few questions yourself.

By phone

- Ask for the correct spelling of the caller's name.
- Ask for a number where you can return the call.
- Ask why the information is needed.

- Ask who has authorized the request and let the caller know that you will verify the authorization.

In Person

- Ask for some identification.
- Ask who has authorized this request so you may verify the authorization.
- If you are not authorized to provide that information, offer to locate the correct person.
- Seek assistance if you are unsure.

Software Piracy

Violating software licensing can result in hefty fines and negative publicity. Understanding some basic licensing methods and adhering to the guidelines that follow can help to ensure that our organization does not contribute to software piracy.

There are three broad categories of software licenses.

Freeware: Software that may be freely copied, shared and used. The author often restricts altering or using it as a component of other software.

Shareware: Software that may be freely copied and shared but used only for the trial period or use stated at which point a registration fee must be paid to continue its use or to enable advanced features.

Commercial: Software that must be purchased before any use and allows for either one installation per purchased copy (a retail license), a negotiated number of installations (a corporate license) or installation on all computers within an organization (a site license).

- Only obtain software through approved methods.
- Install software in accordance with its licensing.
- Don't share software with others.
- Maintain receipts for purchased software.
- Do not illegally copy software.
- Always credit referenced sources properly.
- Do not reproduce copyrighted material without written permission.

Spam

Spam is basically unsolicited and usually unwanted e-mail that you may receive. It is usually a form of advertisement for anything from get-rich-quick schemes to pornography sites on the Internet.

The simplest thing to do with most spam messages is just hit the delete key - end of story. If the problem is persistent or you notice a lot of messages coming from the same source, contact the appropriate person to block this source and register a complaint with the originating Internet service provider.

Telephone Fraud

Unauthorized access to a phone system or phone account number can result in a financial nightmare. It takes only minutes to begin accumulating thousands of dollars in charges to a compromised phone system or calling card.

There are three basic areas of telephone fraud and ways you can prevent it.

- Toll fraud
 - Be sure you know where you are transferring callers.
 - Do not transfer unknown callers to an outside line.
 - Use strong voice mail passwords.
 - Verify area codes before calling unknown numbers.

- Calling card fraud or theft
 - When using a public phone, shield the number pad as you enter your calling card number.
 - If a pay phone rings as you are about to pick it up, use a different phone or wait until a few minutes after the phone stops ringing.
 - Do not give your calling card number over the phone to an unknown caller. Ask for a number to return the call. Call your local phone company's customer service department and report the incident.
 - Always review your monthly phone bill for accuracy and be sure to report any suspicious activity to your phone company.

- Cell phone fraud or theft
 - Avoid leaving your cell phone unattended and place it out of sight if leaving it in a vehicle.
 - Using the lock code on your phone can help limit the amount of fraudulent calls charged to your phone should it be stolen.
 - Cellular phones have an internally unique number referred to as the Electronic Serial Number (ESN). If someone obtains your ESN they could reprogram another phone with it and make calls that would be billed to your account.
 - Store your service agreement (which usually contains your ESN) in a safe place.

Viruses

A computer virus is a self-replicating, usually malicious program segment that attaches itself to a legitimate application or other executable program. The objective of viruses can range from harmless proliferation to sudden, time-triggered, widespread destruction of data.

- Always use anti-virus software on your computer. A free 30 day copy of NOD 32 can be found at <http://eset.com.au/>
- Make sure your anti-virus software is current

- Scan all files downloaded from the Internet
- Scan all email attachments
- Scan diskettes and CDs before use
- Remember, whenever there's a doubt, scan it!
- Report all virus incidents as soon as possible. If you have a computer virus threat to report, please email support@ediscoverytools.com.

What If I Have A Virus?

If you're using your anti-virus software as you should and it does detect a virus, don't panic. In most cases, the software will be able to remove the virus by itself. Even if it does, you should report the incident immediately so that the source can be traced and anyone else who may have received the virus can be alerted. If you don't, it just might find its way back to you!

If your software cannot remove the virus, leave the computer as it is and email the Help Desk for technical support.

Need Additional Guidance?

- Contact support@ediscoverytools.com