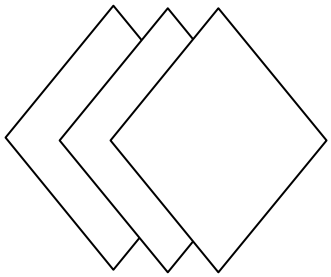
Data Security policy.



DISABILITY INQUISITION ACTIVITIES (DIA).

Bishoykhali Bazar.
P.O-Kharikhali-7300, Jhenaidah, Bangladesh.
Mobile: +8801711-278665,
E-mail: dia.ngo274@gmail.com
Website: www.dia.org.bd

B.M; Nazmul Hasan
President (DIA)
Bishoykhali Bazar, Jhenaidah

Md, Rofikul Islam
Executive Director (DIA)
Bishoykhali Bazar, Jhenaidah

DATA SECURITY TOOLKIT :

When planning your backup system, budget may be a factor in deciding which route you take. However, you have to pick a system you will use. Saving money isn't a value if it's tedious work that never actually gets done and you don't have a current backup when you need it. Your backup policy should include determination for how long backup copies will be kept. Additional USB drives can be purchased to maintain offsite backups. If using the tape system, have a series of tapes that you rotate. Because tapes deteriorate, replace them on a regular basis to prevent problems. Keeping end of month or end of year backups offsite may be helpful as well.

W Password Security:

Recent headlines highlight the continued problem of creating simple passwords that are quickly hacked because they are easier to remember. If a site requires a complicated password, some people will write it down and attach the post-it note to their computer so they have easy access to it when they need it. Others save a document in the system with their list of passwords to various sites. Any of these methods are hazards that can provide unauthorized access to your system. To combat the dangers of password accessibility, provide minimum requirements of at least eight characters and combinations of the following:
lowercase letters, uppercase letters, numbers, and special characters. Simple common rods or the individual's name and date of birth should be prohibited. Provide some examples of possible strong passwords that would be easy to remember, such as word combinations (previous addresses: Main#202ParkDrive). Passwords should be scheduled to be changed on a regular basis, and passwords should not be able to be used over and over again in succession. In addition to making sure individual passwords are truly secure, be sure that the system passwords for wireless access and other equipment are also changed. These hidden passwords can open up the entire system to hackers even if you think you've created a secure system with layers of access.

X Internet Use:

Preventing employees from ever surfing to a network- related website can be cost prohibitive for small and medium sized firms. However, having a clear internet use policy can help limit the types of sites they visit. Streaming music and video use a lot of bandwidth, and downloaded files from file sharing sites can contain malware or expose the firm to liability if material was copyrighted. Some employees may be tempted to spend too much time on activities such as online shopping, social media or travel planning, again, use the theory that if it isn't forbidden, they will do it. Specifically list any types of sites that you do not want your employees visiting on your office computer. Security settings can be set to block porn sites, gambling sites, social media and even web based email sites. The logic behind blocking personal, web-based email is prevention of employees from opening emails and visiting a nefarious site or opening an infected attachment, thereby compromising your system because their personal email was not as secure. Employees may inadvertently or maliciously transmit client confidential or law firm proprietary information using their personal webmail, circumventing other safeguards the firm has established concerning such information. Remind employees that, like email, browsing history is subject to being reviewed.

B.M. Nazmul Hasan
President (DIA)
Bishoykhali Bazar, Jhenaidah

Md, Rofikul Islam
Executive Director (DIA)
Bishoykhali Bazar, Jhenaidah

y E-mail:

Misuse of company email is one of the most common problems faced, and covers a large variety of actions. Sending a free “Happy Birthday!” card from a free website can introduce massive spamming into your system and bog down your server. Employees may use company e-mail for running a personal business with less thought than storing hard files on the computers or servers. A good Samaritan employee may send out emails to everyone in the firm regarding a fundraising event for a local charity, and follow up with four or five reminders. Personal use of the firm email system should be addressed to reduce the amount of server space such items consume. E-mail policies should also include limits on the size of attachments as appropriate. Consider this: an e-mail with a 10MB attachment is received and then forwarded to ten other employees. This attachment now consumes 120MB of server space as each individual copy of the e-mail is stored on the server, plus the copy in the sent folder. Depending on your e-mail client, a copy of the e-mail may also be stored on each and every computer. The above space consumption issue illustrates the reasoning behind another policy: e-mail retention policy. Case-related e-mails and attachments should be uploaded into a practice management system or database, protecting them from accidental deletion and making them accessible to all employees who may need the information. Storing emails that need to be saved outside of the e-mail system also prevents the dreaded moment when the recipient is out of the office and IT has to search their e-mail so another employee can access the information. An essential element of an e-mail policy is reminding employees that the office email system is firm property and not their personal account. As such, any office email account is subject to review. Remind employees that office e-mail is representative of the firm and should present a professional image.

z Metadata:

Perhaps the most overlooked data security danger is metadata contained in document editing programs. Both Microsoft Word and WordPerfect contain information regarding previous edits made to a document. This means that deleting confidential information from one client document to reuse for

another could expose the former client’s information to the latter if the recipient knows where to look. These features can be turned off, preventing data from being stored in the first place. Files sent electronically should be scrubbed for metadata. Special programs can be purchased to ensure that this information is not forwarded along with your document and can be integrated into your email system. If you do not want the recipient to make changes to your document, send the document as a PDF. Sending as a PDF strips most of the metadata from a file, but a PDF contains some of its own. Be sure to adjust the security options as appropriate.

Remote Access:

Employees may need to access the firm’s system when they are out of the office occasionally. Prohibiting employees from using public computers or using wireless access in public places removes the exposure of client data from hackers because security settings in these circumstances are often lower than those created for the office. To make connecting to the office more secure, consider establishing a virtual private network (VPN). A VPN connects you to your office computer over the internet, alleviating the need to actually access files through a questionable internet connection. Communications sent through the VPN are encrypted, so any data intercepted would not be usable.

B.M. Nazmul Hasan
President (DIA)
Bishoykhali Bazar, Jhenaidah

Md, Rofikul Islam
Executive Director (DIA)
Bishoykhali Bazar, Jhenaidah

Smartphones, Tablets and Remote Storage Devices:

The trickiest part of data security is protecting the mobile data that leaves the building. Smartphones and tablets all contain internet connections but often do not have all of their security measures activated as a firm laptop would provide. A USB drive often contains pure, unencrypted files available for anyone who plugs the drive into their computer; worse yet, it is small enough to easily lose. Any device used to access client data should have password protection requirements. Even a USB device can be purchased that requires password access. For smartphones and tablets, require passwords at start up and after a period of idle time. Also, develop a remote wipe program protocol should any device ever be lost or stolen. Any document downloaded and stored should be encrypted. When travelling, be careful not to leave your device in 'airplane mode' as this often disables the ability to enact a remote wipe program as it disconnects the device from data systems used to locate it. Upon return to the office, require that remote storage devices such as USB and flash drives be scanned by virus and malware scanners to prevent infection from any outside sources. Have protocols in place regarding the use of personal USB devices with office computers to avoid inadvertently infecting office computers with unprotected devices. Consider restricting access to USB ports to certain employees, or even disable ports to prevent misuse.

When an Employee Leaves :

Often the biggest threat to your data is within your own company. A disgruntled or exiting employee can easily delete files from your system or take files out of the office without notice. Locking down data from employees can be the hardest part of data security. When an employee leaves, immediately lock their computer, e-mail, remote access and any other access privilege to prevent them from accessing information. Create protocols within the firm for who may need to access an employee's files. If the employee has any equipment, such as a laptop or USB drive, at home, verify that it is returned before they exit the premises on their final day.

Visitors and Contractors:

From time to time, office visitors may need to use office computers or email. Any temporary account established should have a notice regarding expectation of privacy. Passcodes for these accounts should also expire immediately after use. This ensures someone temporarily allowed into your system won't be able to access your confidential data later, when you're not looking. System contractors obviously need access to keep everything up-to-date and running smoothly. However, they may not understand the importance of the confidentiality of the information they may access in the process of completing their work. A Vendor/ Contractor Confidentiality Agreement should be completed by all of those who will be accessing your system to ensure that confidentiality is maintained.

Security Audit:

To ensure all facets of your system are properly secure, consider a third party security audit. A trained professional will see any holes in your protection that could leak confidential information. The auditor will be able to provide you with suggestions to improve your security to prevent data security breaches in the future. This may include the purchase of additional security software, or simply changing internet usage habits. The end result will be a safer practice.

B.M; Nazmul Hasan
President (DIA)
Bishoykhali Bazar, Jhenaidah

Md, Rofikul Islam
Executive Director (DIA)
Bishoykhali Bazar, Jhenaidah

I. Overview

a. **Purpose** –

"Disability Inquisition Activities (DIA)" is entrusted with the responsibility to provide professional legal advice to clients who provide us with confidential information. Inherent in this responsibility is an obligation to provide appropriate protection against theft of data and malware threats, such as viruses and spyware applications. The purpose of this policy is to establish standards for the base configuration of equipment that is owned and/or operated by **"**Disability Inquisition Activities (DIA)" or equipment that accesses "Disability Inquisition Activities(DIA)'s internal systems. Effective implementation of this policy will minimize unauthorized access to "Disability Inquisition Activities **(**DIA)" proprietary information and technology and protect confidential client information.

b. Scope –

This policy applies to equipment owned and/or operated by "Disability Inquisition Activities (DIA)", and to employees connecting to any "Disability Inquisition Activities (DIA)" -owned network domain.

II. Network/Server Security

a. Server Configuration Guidelines

i. The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
ii. Servers should be physically located in an access-controlled environment.
iii. Servers are specifically prohibited from being operated from uncontrolled cubicle areas.

b. **Security-related Events** –

Security-related events will be reported to the IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

i. Port-scan attacks
ii. Evidence of unauthorized access to privileged accounts
iii. Anomalous occurrences that are not related to specific applications on the host.

c. Router Security

i. The enable password on the router must be kept in a secure encrypted form. The router must have the enable password set to the current production router password from the router's support organization.
ii. Disallow the following:

1. IP directed broadcasts
2. Incoming packets at the router sourced with invalid addresses such as RFC1918 address
3. TCP small services
4. UDP small services
5. All source routing
6. Web services running on router

iii. Access rules are to be added as business needs arise.
iv. Each router must have the following statement posted in clear view: "UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device.

B.M; Nazmul Hasan
President (DIA)
Bishoykhali Bazar, Jhenaidah

Md, Rofikul Islam
Executive Director (DIA)
Bishoykhali Bazar, Jhenaidah

d. Server Malware Protection

i. Anti-Virus - All servers MUST have an anti-virus application installed that offers real-time scanning protection to files and applications running on the target system if they meet one or more of the following conditions:
1. Non-administrative users have remote access capability
2. The system is a file server
3. Share access is open to this server from systems used by non-administrative users
4. HTTP/FTP access is open from the Internet

5. Other "risky" protocols/applications are available to this system from the Internet at the discretion of the "Disability Inquisition Activities (DIA)" IT department.
ii. Mail Server Anti-Virus - If the target system is a mail server it MUST have either an external or internal anti-virus scanning application that scans all mail destined to and from the mail server. Local anti-virus scanning applications MAY be disabled during backups if an external anti-virus application still scans inbound e-mails while the backup is being performed.
iii. Anti-Spyware - All servers MUST have an anti-spyware application installed that offers real-time protection to the target system if they meet one or more of the following conditions:
1. Any system where non-technical or non-administrative users have remote access to the system and ANY outbound access is permitted to the Internet
2. Any system where non-technical or non-administrative users have the ability to install software on their own
iv. Notable Exceptions - Exceptions to above requirements may be deemed acceptable with proper Documentation if one of the following notable conditions applies to this system:
1. The system is a SQL server
2. The system is used as a dedicated mail server
3. The system is not a Windows based platform
e. Backup Procedures
i. Daily Backups - Backup software shall be scheduled to run nightly to capture all data from the previous day.
1. B backup logs are to be reviewed to verify that the backup was successfully completed.
2. One responsible party should be available to supervise backups each day. If the designated backup specialist is not available, an alternative should be named to oversee the process.
ii. Backup data storage shall not be on the "Disability Inquisition Activities (DIA)"premises. In case of a disaster, backup tapes should be available for retrieval and not subject to destruction.
iii. Data on hard drives will be backed up daily, and mobile devices shall be brought in to be backed up on a weekly basis or as soon as practical if on an extended travel arrangement.
iv. Test restoration process regularly and create written instructions in the event IT personnel are not available to restore data when needed.

III. Workstation Security

a. Authorized Users - Appropriate measures must be taken when using workstations to ensure the Confidentiality, integrity and availability of sensitive information is restricted to authorized users.
b. Safeguards "Disability Inquisition Activities (DIA)" will implement physical and technical safeguards for all workstations that access electronic confidential information to restrict access to authorized users. Appropriate measures include:
i. Restricting physical access to workstations to only authorized personnel.
ii. Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.
iii. Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected.

B.M; Nazmul Hasan
President (DIA)
Bishoykhali Bazar, Jhenaidah

Md, Rofikul Islam
Executive Director (DIA)
Bishoykhali Bazar, Jhenaidah

iv. Complying with all applicable password policies and procedures.
v. Ensuring workstations are used for authorized business purposes only
vi. Never installing unauthorized software on workstations.
vii. Storing all confidential information on network servers.
viii. Keeping food and drink away from workstations in order to avoid accidental spills.
ix. Securing laptops that contain sensitive information by using cable locks or locking laptops up in drawers or cabinets.
x. Complying with the Portable Workstation Encryption policy.
xi. Complying with the Anti-Virus policy.
xii. Ensuring that monitors are positioned away from public view. If necessary, install privacy screen filters or other physical barriers to public viewing.
xiii. Ensuring workstations are left on but logged off in order to facilitate after-hours updates. Exit running applications and close open documents.
xiv. Ensuring that all workstations use a surge protector (not just a power strip) or a UPS (battery backup).
xv. If wireless network access is used, ensure access is secure by following the Wireless Access policy.

c. Software Installation
i. Employees may not install software on "Disability Inquisition Activities (DIA)" computing devices operated within the "Disability Inquisition Activities (DIA)" network. Software requests must first be approved by the requester's manager and then be made to the IT department in writing or via e-mail. Software must be selected from an approved software list, maintained by the IT department, unless no selection on the list meets the requester's need. The IT department will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation.
ii. This policy covers all computers, servers, and other computing devices operating within "Disability Inquisition Activities (DIA)'s network.
d. Malware Protection
i. Anti-Virus – All computers must have "Disability Inquisition Activities (DIA)'s standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date. Virus-infected computers must be removed from the network until they are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into **"**Disability Inquisition Activities (DIA)'s networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited, in accordance with the Acceptable Use policy.

IV. Password Security

a. Requirements
i. All system-level passwords (Administrator, etc.) must be changed on a quarterly basis, at a minimum.
ii. All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months.
iii. All user-level and system-level passwords must conform to the standards described below.
b. Standards - All users at **"**Disability Inquisition Activities (DIA)" should be aware of how to select strong passwords. Strong passwords
have the following characteristics:
i. Contain at least three of the five following character classes:
1. Lower case characters
2. Upper case characters
3. Numbers
4. Punctuation
5. "Special" characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc)
ii. Contain at least eight to fifteen alphanumeric characters.
iii. The password is not a word found in a dictionary (English or foreign).
iv. The password is not a common usage word such as:
1. Computer terms and names, commands, sites, companies, hardware, software. Passwords should NEVER be "Password1" or any derivation.

B.M; Nazmul Hasan
President (DIA)
Bishoykhali Bazar, Jhenaidah

Md, Rofikul Islam
Executive Director (DIA)
Bishoykhali Bazar, Jhenaidah

2. The words "Disability Inquisition Activities (DIA)", JHENAIDAH", or any derivation.
3. Names of family, pets, friends, co-workers, etc.

4. Birthdays and other personal information such as addresses and phone numbers.
5. Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
6. Any of the above spelled backwards.
7. Any of the above preceded or followed by a digit (e.g., secret1, 1secret).
v. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase.
c. Protective Measures
i. Do not share **"**Disability Inquisition Activities (DIA)" passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential **"**Disability Inquisition Activities (DIA)" information.
ii. Passwords should never be written down or stored on-line without encryption.
iii. Do not reveal a password in email, chat, or other electronic communication.
iv. Do not speak about a password in front of others.
v. Do not hint at the format of a password (e.g., "my family name").
vi. Do not reveal a password on questionnaires or security forms.
vii. If someone demands a password, refer them to this document and direct them to the IT Department.
viii. Always decline the use of the "Remember Password" feature of applications.
d. Passphrases - Access to the "Disability Inquisition Activities (DIA)" Networks via remote access is to be controlled using either a onetime password authentication or a public/private key system with a strong passphrase.
i. A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase: "Joe&Me1RBudz"
ii. All of the rules above that apply to passwords apply to passphrases.

V. Acceptable Use

a. General Use and Ownership
i. While "Disability Inquisition Activities (DIA)'s network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of "Disability Inquisition Activities (DIA).
ii. Any information that users consider sensitive or vulnerable be encrypted.
iii. For security and network maintenance purposes, authorized individuals within "Disability Inquisition Activities (DIA)" may monitor equipment, systems and network traffic at any time.
b. Security and Proprietary Information
i. The user interface for information contained on "Disability Inquisition Activities (DIA)'s systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines. Employees should take all necessary steps to prevent unauthorized access to this information.
ii. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly, user level passwords should be changed every six months.
iii. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when unattended.
iv. All PCs, laptops and workstations used by the employee that are connected to the "Disability Inquisition Activities(DIA)" network, whether owned by the employee or "Disability Inquisition Activities(DIA)", shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.
v. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.
c. Unacceptable Use
i. T he following activities are, in general, prohibited. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

B.M; Nazmul Hasan
President (DIA)
Bishoykhali Bazar, Jhenaidah

Md, Rofikul Islam
Executive Director (DIA)
Bishoykhali Bazar, Jhenaidah

1. Under no circumstances is an employee of "Disability Inquisition Activities (DIA)" authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing "Disability Inquisition Activities(DIA)" owned resources.
2. Violations of the rights of any person or Firm protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by "Disability Inquisition Activities(DIA)".
3. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which <Firm Name> or the end user does not have an active license is strictly prohibited.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
7. Using a **"**Disability Inquisition Activities (DIA)"computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
8. Making fraudulent offers of products, items, or services originating from **"**Disability Inquisition Activities (DIA)"account.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification to the IT department is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet.
15. Providing information about, or lists of, "Disability Inquisition Activities (DIA)"employees to parties outside "Disability Inquisition Activities (DIA)"

d. Wireless Access

i. "Disability Inquisition Activities (DIA)"Device Requirements - All wireless devices that reside at a "Disability Inquisition Activities (DIA)"site and connect to a "Disability Inquisition Activities **(**DIA)"network must:

1. B e installed, supported, and maintained by the IT department.
2. Use "Disability Inquisition Activities (DIA)" approved authentication protocols and infrastructure.
3. Use "Disability Inquisition Activities (DIA)"approved encryption protocols.
4. Maintain a hardware address (MAC address) that can be registered and tracked.

ii. Home Wireless Device Requirements

1. Wireless devices that provide direct access to the "Disability Inquisition Activities **(**DIA)"corporate network, must conform

B.M; Nazmul Hasan
President (DIA)
Bishoykhali Bazar, Jhenaidah

Md, Rofikul Islam
Executive Director (DIA)
Bishoykhali Bazar, Jhenaidah

to the security protocols as detailed for "Disability Inquisition Activities (DIA)"wireless devices.
2. Wireless devices that fail to conform to security protocols must be installed in a manner that prohibits direct access to the "Disability Inquisition Activities (DIA)"corporate network. Access to the "Disability Inquisition Activities (DIA)"
corporate network through this device must use standard remote access authentication.

VI. Encryption.

a. Standards - Proven, standard algorithms should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. Key lengths must be at least 128 bits. "Disability Inquisition Activities (DIA)'s key length requirements will be reviewed annually and upgraded as technology allows.
b. Mobile Device Encryption
i. Scope - All mobile devices containing stored data owned by <Firm Name> must use an approved method of encryption to protect data at rest. Mobile devices are defined to include laptops, tablets, and smart phones.
ii. Laptops - Laptops must employ full disk encryption with an approved software encryption package. No "Disability Inquisition Activities (DIA)" data may exist on a laptop in clear text.
iii. Tablet and smartphones - Any "Disability Inquisition Activities (DIA)**"** data stored on a smartphone or tablet must be saved to an encrypted file system using "Disability Inquisition Activities (DIA)"approved software. "Disability Inquisition Activities (DIA)"shall also employ remote wipe technology to remotely disable and delete any data stored on a "Disability Inquisition Activities (DIA)"tablet or smartphone which is reported lost or stolen.
iv. Keys - All keys used for encryption and decryption must meet complexity requirements described in "Disability Inquisition Activities (DIA)'s Password Security policy.

VII. E-mail

a. Prohibited Use - "Disability Inquisition Activities (DIA)"e-mail system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any e-mails with this content from any "Disability Inquisition Activities (DIA)" employee should report the matter to their supervisor immediately. The following activities are strictly prohibited, with no exceptions:
i. Sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (e-mail spam).
ii. Any form of harassment via e-mail, telephone or paging, whether through language, frequency, or size of messages.
iii. Unauthorized use, or forging, of e-mail header information.
iv. Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies.
v. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
vi. Use of unsolicited e-mail originating from within "Disability Inquisition Activities (DIA)'s networks of other Internet/Intranet/ Extranet service providers on behalf of, or to advertise, any service hosted by "Disability Inquisition Activities (DIA)"or connected via "Disability Inquisition Activities (DIA)'s network.
vii. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
b. Personal Use - Using a reasonable amount of **"**Disability Inquisition Activities (DIA)"resources for personal e-mails is acceptable, but no work related e-mail shall be saved in a separate folder from work related e-mail. Sending chain letters or joke e-mails from a "Disability Inquisition Activities (DIA)'e-mail account is prohibited. Virus or other malware warnings and mass mailings from "Disability Inquisition Activities (DIA)" shall be approved by "Disability Inquisition Activities (DIA)"IT department before sending. These restrictions also apply to the forwarding of mail received by "Disability Inquisition Activities (DIA)"employee.

B.M; Nazmul Hasan
President (DIA)
Bishoykhali Bazar, Jhenaidah

Md, Rofikul Islam
Executive Director (DIA)
Bishoykhali Bazar, Jhenaidah

c. E-mail Retention

i. Administrative Correspondence - "Disability Inquisition Activities (DIA)"Administrative Correspondence includes, though is not limited to clarification of established Firm policy, including holidays, time card information, dress code, work place behavior and any legal issues such as intellectual property violations. All e-mail with the information sensitivity label Management Only shall be treated as Administrative Correspondence. "Disability Inquisition Activities (DIA)"Administration is responsible for e-mail retention of Administrative Correspondence.
ii. Fiscal Correspondence - "Disability Inquisition Activities (DIA)"Fiscal Correspondence is all information related to revenue and expense for the Firm "Disability Inquisition Activities (DIA)"bookkeeper is responsible for all fiscal correspondence.
iii. General Correspondence - **"**Disability Inquisition Activities (DIA)"General Correspondence covers information that relates to customer interaction and the operational decisions of the business. "Disability Inquisition Activities (DIA)"is responsible for e-mail retention of General Correspondence.
iv. Ephemeral Correspondence - "Disability Inquisition Activities (DIA)"Ephemeral Correspondence is by far the largest category and includes personal e-mail, requests for recommendations or review, e-mail related to product development, updates and status reports.
v. Encrypted Communications - "Disability Inquisition Activities (DIA)"encrypted communications should be stored in a manner that protects the confidentiality of the information, but in general, information should be stored in a decrypted format.
vi. Recovering Deleted E-mail via Backup Media - "Disability Inquisition Activities (DIA)"maintains backups from the e-mail server and once a quarter a set of backups is taken out of the rotation and they are moved offsite. No effort will be made to remove e-mail from the offsite backups.
d. Monitoring - "Disability Inquisition Activities (DIA)"employees shall have no expectation of privacy in anything they store, send or receive on the Firm's e-mail system. "Disability Inquisition Activities (DIA)"may monitor messages without prior notice. "Disability Inquisition Activities (DIA)" is not obliged to monitor e-mail messages.

VIII. Metadata

a. Definition - When you create and edit your documents, information about you and the edits you make is automatically created and hidden within the document file. Metadata can often be sensitive or confidential information, and can be potentially damaging or embarrassing. On its Web site, Microsoft indicates that the following metadata may be stored in documents created in all versions of Word, Excel and PowerPoint:
i. your name and initials (or those of the person who created the file)
ii. the name of your computer
iii. your firm or organization name
iv. the name and type of the printer you printed the document on
v. document revisions, including deleted text that is no longer visible on the screen
vi. document versions
vii. information about any template used to create the file
viii. hidden text
ix. comments
b. Removing Metadata
i. Microsoft
1. Disable "allow fast saves" feature.
2. "Inspect Document" and remove flagged items. "Inspect Document" will vary depending on your software version. In 2010, it is located under File->Info->Check For issues.
3. Third party software will help identify and clean metadata from your documents if it is necessary to send documents in native format. Verify appropriate software with the IT department.
ii. WordPerfect

B.M; Nazmul Hasan
President (DIA)
Bishoykhali Bazar, Jhenaidah

Md, Rofikul Islam
Executive Director (DIA)
Bishoykhali Bazar, Jhenaidah

DATA SECURITY TOOLKIT

1. Uncheck Save Undo/Redo items with document. It can allow you to view hundreds of past changes in terms of what text was cut, copied and even deleted from the document.
2. T here is no software program that easily and automatically removes metadata from WordPerfect documents.
iii. Converting to PDF
1. Converting files to PDF format with Adobe Acrobat or other PDF creators will usually strip out most metadata.
2. In Acrobat, Select File, then Document Properties to view the summary metadata information within a PDF file. Add further restrictions on how the document can be accessed, used, copied and printed in the Security Options settings as needed.

IX. R emote Access

a. Persons Affected - "Disability Inquisition Activities (DIA)"employees, consultants, vendors, contractors, students, and others who use mobile computing and storage devices on the network at the "Disability Inquisition Activities (DIA)"
b. General Standards - It is the responsibility of "Disability Inquisition Activities (DIA)"employees, contractors, vendors and agents with remote access privileges to "Disability Inquisition Activities (DIA)'s corporate network to ensure that their remote access connection
is given the same consideration as the user's on-site connection to "Disability Inquisition Activities (DIA)"
c. Requirements
i. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong passphrase see the Password policy.
ii. At no time should any "Disability Inquisition Activities (DIA)"employee provide their login or e-mail password to anyone, not even family members.
iii. "Disability Inquisition Activities (DIA)"employees and contractors with remote access privileges must ensure that their "Disability Inquisition Activities (DIA)"owned or personal computer or workstation, which is remotely connected to "Disability Inquisition Activities (DIA)'s corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
iv. "Disability Inquisition Activities (DIA)"employees and contractors with remote access privileges to "Disability Inquisition Activities (DIA)"'s corporate network must not use non "Disability Inquisition Activities (DIA)" e-mail accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct "Disability Inquisition Activities (DIA)"business, thereby ensuring that official business is never confused with personal business.
v. Routers configured for access to the "Disability Inquisition Activities (DIA)"network must meet minimum authentication requirements .
vi. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
vii. Non-standard hardware configurations must be approved by the IT department, and "Disability Inquisition Activities (DIA)"must approve security configurations for access to hardware.
viii. All PCs, laptops and workstations that are connected to "Disability Inquisition Activities (DIA)"internal networks via remote access technologies must use the most up-to-date anti-virus software (place URL to corporate software site here), this includes personal computers.
ix. Personal equipment that is used to connect to "Disability Inquisition Activities (DIA)"'s networks must meet the requirements of "Disability Inquisition Activities (DIA)"owned equipment for remote access.

B.M; Nazmul Hasan
President (DIA)
Bishoykhali Bazar, Jhenaidah

Md, Rofikul Islam
Executive Director (DIA)
Bishoykhali Bazar, Jhenaidah

x. Individuals who wish to implement non-standard Remote Access solutions to the "Disability Inquisition Activities (DIA)" production network must obtain prior approval from the IT department.

d. Mobile Computing and Storage Devices

i. Items covered - Mobile computing and storage devices include, but are not limited to: laptop computers, plug-ins, Universal Serial Bus (USB) port devices, Compact Discs (CDs), Digital Versatile Discs (DVDs), flash drives, smartphones, tablets, wireless networking cards, and any other existing or future mobile computing or storage device, either personally owned or "Disability Inquisition Activities (DIA)" owned, that may connect to or access the information systems at the "Disability Inquisition Activities (DIA)".

ii. Risks - Mobile computing and storage devices are easily lost or stolen, presenting a high risk for Unauthorized access and introduction of malicious software to the network at the "Disability Inquisition Activities (DIA).These risks must be mitigated to acceptable levels.

iii. Encryption - Portable computing devices and portable electronic storage media that contain confidential, personal, or sensitive "Disability Inquisition Activities (DIA)"information must use encryption or equally strong measures to protect the data while it is being stored.

iv. Database - Databases or portions thereof, which reside on the network at the "Disability Inquisition Activities (DIA)", shall not be downloaded to mobile computing or storage devices.

v. Minimum Requirements:

1. Report lost or stolen mobile computing and storage devices to the IT department.
2. Non-departmental owned device that may connect to the "Disability Inquisition Activities (DIA)" network must first be approved by the IT department.
3. Compliance with the Remote Access policy is mandatory.

e. Virtual Private Network (VPN)

i. Persons affected - This policy applies to all "Disability Inquisition Activities (DIA)"employees, contractors, consultants,

Temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the "Disability Inquisition Activities (DIA)"network.

ii. Connectivity - Approved "Disability Inquisition Activities (DIA)"employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees.

iii. Requirements

1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to "Disability Inquisition Activities (DIA)"internal networks.
2. VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.
3. When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
4. Dual (split) tunneling is NOT permitted; only one network connection is allowed.
5. VPN gateways will be set up and managed by "Disability Inquisition Activities (DIA)'s IT department.
6. All computers connected to "Disability Inquisition Activities (DIA)"internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard (provide URL to this software); this includes personal computers.
7. VPN users will be automatically disconnected from "Disability Inquisition Activities (DIA)"s network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
8. T he VPN concentrator is limited to an absolute connection time of 24 hours.
9. Users of computers that are not "Disability Inquisition Activities (DIA)"owned equipment must configure the equipment to comply with "Disability Inquisition Activities (DIA)'s VPN and Network policies.
10. Only "Disability Inquisition Activities (DIA)"approved VPN clients may be used.

B.M; Nazmul Hasan
President (DIA)
Bishoykhali Bazar, Jhenaidah

Md, Rofikul Islam
Executive Director (DIA)
Bishoykhali Bazar, Jhenaidah

11. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of "Disability Inquisition Activities (DIA)'s network, and as such are subject to the same rules and

regulations that apply to "Disability Inquisition Activities (DIA)"owned equipment, i.e., their machines must be configured to comply with "Disability Inquisition Activities (DIA)'s Security Policies.

X. Employee Termination

a. Removing access - An employee's credentials shall be inactivated immediately upon termination of employment. This includes, but is not limited to the following:

i. "Disability Inquisition Activities (DIA)"database

ii. Workstation access

iii. E-mail access

iv. Remote access to **"**Disability Inquisition Activities (DIA)'s network

v. VPN client access

vi. Any other access to **"**Disability Inquisition Activities (DIA)"network or programs

b. Returning mobile devices - Any employee in possession of firm portable devices shall return such devices before exiting the premises on their final day of employment. Mobile devices include, but are not limited to, the following:

i. "Disability Inquisition Activities (DIA)"owned smartphone

ii. "Disability Inquisition Activities (DIA)"owned tablet

iii. Laptop

iv. USB drive

v. CD or DVD containing "Disability Inquisition Activities (DIA)"client information

XI. Visitor and Contractor Access

a. Permission - Visitors who require internet network access will need permission the IT department. After credentials are arranged, activities on the network will be subject to the Acceptable Use policy. Visitor use of employee credentials is not permitted under any circumstances.

b. Contractors - Contractors making changes to the network should notify the IT department if any interruption of services is anticipated. Prior arrangement should be made to notify all staff of the interruption if possible.

c. Remote Access - Remote Access to "Disability Inquisition Activities (DIA)"networks are governed by the "Disability Inquisition Activities (DIA)"s Remote Access policy.

XII. Enforcement

a. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

SERVICE PROVIDE R CONFIDENTIALITY AG REEMENT.

It is the policy and practice of "Disability Inquisition Activities (DIA)"that the confidentiality of all client, law office business and related matters is carefully guarded and protected in every possible and reasonable manner at all times. For that reason, you are being asked in your capacity as an employee or representative of "X ", a service provider to "the firm" (hereinafter "X") to review and sign this confidentiality form. Your signature below represents and documents your acknowledgement and agreement to maintain complete and strict confidentiality regarding any client information and any and all other office matters that you may be told or inadvertently or otherwise learn in the course of your work with "Law Firm." Any breach of this confidentiality policy to third parties will result in the immediate termination of our business relationship. Further, should you breach this confidentiality policy in any way, you and your company will be jointly and severally liable for any and all damages and expenses including attorney fees cause to "the firm," its clients or employees I, "Disability Inquisition Activities (DIA), am an employee and authorized representative for "X" and have read, understand and agree to abide by the provisions of the foregoing stated policy.

B.M; Nazmul Hasan
President (DIA)
Bishoykhali Bazar, Jhenaidah

Md, Rofikul Islam
Executive Director (DIA)
Bishoykhali Bazar, Jhenaidah