Data Security Policy

Last Update Status: *Updated November 2024*

Overview

The purpose of this policy is to establish standards for the base configuration of equipment that is owned and/or operated by or equipment that accesses ToGGeL's (hereinafter "the Firm") internal systems. Effective implementation of this policy will minimize unauthorized access to proprietary information and technology and protect confidential and or personal client information.

Scope

This policy applies to equipment owned and/or operated by ToGGeL, and to employees and/or others connecting to any ToGGeL owned network or domain.

1. Network/Server Security

1.1 Server Configuration Guidelines

1.1.1 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.

1.1.2 Servers should be physically located in an access-controlled environment.

1.1.3 Servers are specifically prohibited from being operated from uncontrolled cubicle areas.

1.1.4 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: (a) Port-scan attacks; (b) Evidence of unauthorised access to privileged accounts; (c) Anomalous occurrences that are not related to specific applications on the host.

1.2 Router security

1.2.1 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 organisation.

1.2.2 Disallow the following:

- IP directed broadcasts
- Incoming packets at the router sourced with invalid addresses such as RFC1918 address
- TCP small services
- UDP small services

- All source routing
- Web services running on router
- Access rules are to be added as business needs arise
- 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."

2. Server Malware Protection

2.1 Anti-Virus software: 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:

2.1.1 Non-administrative users have remote access capability.

2.1.2 The system is a file server.

2.1.3 Share access is open to this server from systems used by non-administrative users.

2.1.4 HTTP/FTP access is open from the Internet.

2.1.5 Other "risky" protocols/applications are available to this system from the Internet at the discretion of the IT department.

2.2 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.

2.3 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:

2.3.1 Any system where non-technical or non-administrative users have remote access to the system and ANY outbound access is permitted to the Internet.

2.3.2 Any system where non-technical or non-administrative users can install software on their own.

2.3.3 Notable Exceptions: Exceptions to the above requirements may be deemed acceptable with proper documentation if one of the following notable conditions applies to this system:

- The system is a SQL server.

- The system is used as a dedicated mail server.
- The system is not a Windows based platform.

3. Backup Procedure

3.1 Daily Backups: Backup software shall be scheduled to run nightly to capture all data from the previous day.

3.2 Backup logs are to be reviewed to verify that the backup was successfully completed.

3.3 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.

3.4 Backup data storage shall not be on the Firm's premises. In case of a disaster, backup tapes should be available for retrieval and not subject to destruction.

3.5 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.

3.6 The IT department will run the Test restoration process regularly and create written instructions in the event IT personnel are not available to restore data when needed.

4. Workstation Security

4.1 Authorised Users: Appropriate measures must be taken when using workstations to ensure that the confidentiality, integrity and availability of sensitive information is restricted to authorised users.

4.2 Safeguards: The IT department will implement physical and technical safeguards for all workstations that access electronic confidential information to restrict access to authorized users. Appropriate measures include:

4.2.1 Restricting physical access to workstations to only authorised personnel.

4.2.2 Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.

4.2.3 Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected.

4.2.4 Complying with all applicable password policies and procedures.

4.2.5 Ensuring workstations are used for authorized business purposes only.

4.2.6 Never installing unauthorized software on workstations.

4.2.7 Storing all confidential information on network servers.

4.2.8 Keeping food and drink away from workstations to avoid accidental spills.

4.2.9 Securing laptops that contain sensitive information by using cable locks or locking laptops up in drawers or cabinets.

4.2.10 Complying with the Portable Workstation Encryption policy.

4.2.11 Complying with the Anti-Virus policy.

4.2.12 Ensuring that monitors are positioned away from public view. If necessary, install privacy screen filters or other physical barriers to public viewing.

4.2.13 Ensuring workstations are left on but logged off to facilitate after-hours updates. Exit running applications and close open documents.

4.2.14 Ensuring that all workstations use a surge protector (not just a power strip) or a UPS (battery backup).

4.2.15 If wireless network access is used, ensure access is secure by following the Wireless Access policy.

4.3 Software Installation

Employees may not install software on computing devices operated within the 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. The IT department will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation. This policy covers all computers, servers, and other computing devices operating within the Firm's network.

5. Malware Protection

Anti-Virus: All computers must have the Firm'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 the Firm's networks (eg viruses) are prohibited, in accordance with the Acceptable Use policy.

6. Password Security Requirements

6.1 All system-level passwords (Administrator, etc.) must be changed on a quarterly basis.

6.2 All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months.

6.3 All user-level and system-level passwords must conform to the standards described below:

6.3.1 Standards: All users at the Firm should be aware of how to select strong passwords. Strong passwords have the following characteristics:

6.3.2 Contain at least three of the five following character classes:

- Lower case characters
- Upper case characters
- Numbers
- Punctuation
- “Special” characters (e.g. @#$%^&*()_+|~-=\`{}[]:”;’<>/ etc)

6.3.3 Contain at least eight to fifteen alphanumeric characters.

6.3.4 The password is NOT a word found in a dictionary (English or foreign).

6.3.5 The password is not a common usage word such as; computer terms and names, commands, sites, companies, hardware, software.

6.3.6 Passwords should NEVER be “Password1” or any derivation. The words “”, “”, or any derivation. Names of family, pets, friends, co-workers, etc. Birthdays and other personal information such as addresses and phone numbers. Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc. Any of the above spelled backwards. Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

6.3.7 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.

6.4 Protective Measures:

6.4.1 Do not share passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential information.

6.4.2 Passwords should never be written down or stored on-line without encryption.

6.4.3 Do not reveal a password in email, chat or other electronic communication.

6.4.4 Do not speak about a password in front of others.

6.4.5 Do not hint at the format of a password (e.g., “my family name”).

6.4.6 Do not reveal a password on questionnaires or security forms.

6.4.7 If someone demands a password, refer them to this document and direct them to the IT Department.

6.4.8 Always decline the use of the “Remember Password” feature of applications.

6.5 Passphrases:

6.5.1 Access to the network via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

6.5.2 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”

6.5.3 All the rules above that apply to passwords apply to passphrases.

6.6 Acceptable Use:

6.6.1 General Use and Ownership. While the Firm’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 the Firm.

6.6.2 Any information that users consider sensitive or vulnerable must be encrypted.

6.6.3 For security and network maintenance purposes, authorized individuals may monitor equipment, systems, and network traffic at any time.

7. Security and Proprietary Information

7.1 The user interface for information contained on the Firm'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.

7.2 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.

7.3 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.

7.4 All PCs, laptops and workstations used by the employee that are connected to the network shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.

7.5 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses and/or malware.

8. **Unacceptable Use**

8.1 The following activities are prohibited:

8.1.1 Under no circumstances is an employee authorised to engage in any activity that is illegal under local, provincial, national or international law while utilising the Firm's resources.

8.1.2 Violations of the rights of any person or the Firm protected by copyright, trade mark, 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 the Firm.

8.1.3 Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the end user does not have an active license is strictly prohibited.

8.1.4 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.

8.1.5 Introduction of malicious programs into the network or server (eg viruses and/or malware).

8.1.6 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.

8.1.7 Using a 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.

8.1.8 Making fraudulent offers of products, items or services originating from any account.

8.2 Effecting security breaches or disruptions of network communication.

8.2.1 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 authorised 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.

8.2.2 Port scanning or security scanning is expressly prohibited unless prior notification s made ito the IT department.

8.2.3 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 duties.

8.2.4 Circumventing user authentication or security of any host, network or account.

8.2.5 Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

8.2.6 Using any program/script/command, or sending messages of any kind with the intent to interfere with, or disable a user's terminal session, by any means, locally or via the Internet.

8.2.7 Providing information about employees to outside parties.

9. Wireless Access

9.1 Device Requirements

All wireless devices that reside at a site and connect to a network must:

- Be installed, supported, and maintained by the IT department.
- Use approved authentication protocols and infrastructure.
- Use approved encryption protocols.
- Maintain a Media Access Control (MAC) address that can be registered and tracked. The MAC adress is a unique 12-digit hexadecimal number that identifies a device on a network.

10. Home Wireless Device Requirements

10.1 Wireless devices that provide direct access to the corporate network, must conform to the security protocols as detailed for wireless devices.

10.2 Wireless devices that fail to conform to security protocols must be installed in a manner that prohibits direct access to the corporate network. Access to the corporate network through this device must use standard remote access authentication.

11. Mobile Device Encryption

11.1 Encryption 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. The Firm's key length requirements will be reviewed annually and upgraded as technology allows.

11.2 Scope

All mobile devices containing stored data owned by the Firm must use an approved method of encryption to protect data. Mobile devices are defined to include laptops, tablets, and smartphones.

11.2.1 Laptops must employ full disk encryption with an approved software encryption package. No data may exist on a laptop in clear text.

11.2.2 Tablets and smartphones: Any data stored on a smartphone or tablet must be saved to an encrypted file system using approved software and shall also employ remote Wipe technology to remotely disable and delete any data stored on a tablet or smartphone which is reported lost or stolen.

11.2.3 Keys: All keys used for encryption and decryption must meet complexity requirements described in the Firm ’s Password Security policy.

12. E-mail

12.1 Prohibited Use

The 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 another employee should report the matter to their supervisor immediately.

The following activities are strictly prohibited:

12.1.1 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).

12.1.2 Any form of harassment via e-mail, telephone, or paging, whether through language, frequency, or size of messages.

12.1.3 Unauthorised use or forging of an e-mail address.

12.1.4 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.

12.1.5 Creating or forwarding “chain letters”, “Ponzi”, "multi-level marketing” or other “pyramid” schemes of any type.

12.1.6 Use of unsolicited e-mail originating from within the Firm's networks of other Internet/Intranet/ Extranet service providers on behalf of, or to advertise, any service hosted by or connected via the Firm 's network.

12.1.7 Posting the same or similar non-business related messages to large numbers of Usenet newsgroups (newsgroup spam).

12.2 Personal Use

Using a reasonable number of resources for personal e-mails is acceptable, but non-work related e-mail shall be saved in a separate folder from work related e-mail. Sending chain letters or joke e-mails from an e-mail account is prohibited. These restrictions also apply to the forwarding of mail received by an employee.

13. E-mail Retention

13.1 Administrative Correspondence

Administrative Correspondence includes, but is not limited to, clarification of established policies such as holidays, timecard information, dress code, workplace behaviour and any legal issues (eg. intellectual property violations). All e-mail with the information sensitivity label "Management Only" shall be treated as Administrative Correspondence. Administration is responsible for e-mail retention of Administrative Correspondence.

13.2 Fiscal Correspondence

Fiscal Correspondence is all the information related to the Firm's revenue and expenditure. The Accountant is responsible for all fiscal correspondence.

13.3 General Correspondence

General Correspondence covers information that relates to customer interaction and the operational decisions of the business. The Operations Manager is responsible for the retention of General Correspondence.

13.4 Ephemeral Correspondence

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.

13.5 Encrypted Communications

Encrypted communications should be stored in a manner that protects the confidentiality of the information.

13.6 Recovering Deleted E-mail via Backup Media

The IT department maintains backups from the e-mail server. Every quarter a set of backups is taken out of rotation and are moved offsite for safekeeping.

13.7 Monitoring

Employees shall have no expectation of privacy regarding information that they store, send or receive on the Firm's e-mail system. The Firm may monitor email messages without prior notice.

14. Metadata

14.1 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:

- your name and initials (or those of the person who created the file)
- the name of your computer
- your firm or organisation's name
- the name and type of printer you print documents on
- document revisions, including deleted text that is no longer visible on the screen
- document versions, information about any template used to create the file
- hidden text
- comments

14.2 Removing Metadata

14.2.1 Microsoft

(a) Disable "allow fast saves" feature.

(b) "Inspect Document" and remove flagged items. "Inspect Document" will vary depending on your software version. In 2010, it was located under File->Info->Check For issues.

(c) 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.

14.2.2 WordPerfect

(a) 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.

(b) There is no software program that easily and automatically removes Metadata from WordPerfect documents.

14.2.3 Converting to PDF

(a) Converting files to PDF format with Adobe Acrobat or other PDF creators will usually strip out most Metadata.

(b) 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.

15. Remote Access

15.1 Persons Affected: Employees, consultants, vendors, contractors, students, and others who use mobile computing and storage devices on the Firms network.

15.2 General Standards: It is the responsibility of employees, contractors, vendors and agents with remote access privileges to the Firm's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection.

15.3 Requirements

15.3.1 Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong passphrases. For information on creating a strong passphrase see the Password policy.

15.3.2 At no time should any employee provide their login or e-mail password to anyone, not even family members.

15.3.3 Employees and contractors with remote access privileges must ensure that their laptop, personal computer or workstation which is remotely connected to the Firm's network is not connected to any other network at the same time.

15.3.4 Employees and contractors with remote access privileges to the Firm ’s corporate network must may use personal e-mail accounts (i.e. Gmail, Hotmail, Yahoo, AOL) or other external resources to conduct business, thereby ensuring that official business is never confused with personal business.

15.3.5 Routers configured for access to the network must meet minimum authentication requirements.

15.3.6 Reconfiguration of a home user’s equipment for the purpose of split-tunneling or dual homing is not permitted.

15.3.7 Non-standard hardware configurations must be approved by the IT department.

15.3.8 All PCs, laptops and workstations that are connected to internal networks via remote access technologies must use the most up-to-date anti-virus software.

15.3.9 Personal equipment that is used to connect to the Firm's network must meet the requirements of personal-owned equipment for remote access.

15.3.10 Individuals who wish to implement non-standard remote access solutions to the Firm's network must obtain prior approval from the IT department.

16. Mobile Computing and Storage Devices

16.1 Items covered

Mobile computing and storage devices include, but are not limited to, laptop computers, Mutual 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 devices that may connect the Firm's network.

16.2 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 Firm's network. These risks must be mitigated to acceptable levels.

16.3 Encryption

Portable computing devices and portable electronic storage media that contain confidential, personal or sensitive information must use encryption or equally strong measures to protect the data while it is being stored.

16.3 Databases

Databases or portions thereof, which reside on the Firm's network shall not be downloaded to mobile computing or storage devices.

16.4 Minimum Requirements

16.4.1 Report lost or stolen mobile computing and storage devices to the IT department.

16.4.2 Non-departmental owned devices that may connect to the Firm's network must be approved by the IT department.

16.4.3 Compliance with the Remote Access policy is mandatory.

17. Virtual Private Network (VPN)

17.1 Persons affected

This policy applies to all employees, contractors, consultants, temporary staff and other workers including all personnel affiliated with third parties utilising VPNs to access the network.

17.2 Connectivity

Approved 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.

17.3 Requirements

It is the responsibility of employees with VPN privileges to ensure that unauthorised users are not allowed access to internal networks.

17.4 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.

17.5 When actively connected to the corporate network all traffic to and from the PC over the VPN tunnel will be dropped.

17.6 Dual (split) tunneling is NOT permitted; only one network connection is allowed.

17.7 VPN gateways will be set up and managed by the Firm's IT department.

17.8 All computers connected to internal networks via VPN, or any other technology, must use the most up-to-date anti-virus software in accordance with the Firm's standards.

17.9 VPN users will be automatically disconnected from the Firm'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.

17.10 The VPN concentrator is limited to an absolute connection time of 24 hours.

17.11 Users of personal devices must configure the equipment to comply with the Firm's VPN and Network policies.

17.12 Only approved VPN clients may be used.

17.13 By using VPN technology with personal equipment users must understand that their machines are a de facto extension of the Firm's network and as such are subject to the same rules and regulations that apply to the Firm's equipment.

18. Employee Termination

18.1 Removing access

An employee's credentials shall be inactivated immediately upon termination of employment. This includes, but is not limited to, the database; workstation; e-mail access; remote access to the Firm's network; VPN client access; another other access to the Firm's network or programs.

18.2 Returning mobile devices

Any employee in possession of the Firm's portable devices shall return such devices before exiting the premises on their final day of employment. Mobile devices include, but are not limited to, smartphones; tablets; laptops; USB drives and CD or DVDs containing client information.

19. Visitor and Contractor Access

19.1 Permission

Visitors who require access to the Firm's network will need permission from the IT department who will issue them with access credentials. Activities on the network will be subject to the Acceptable Use policy. Visitor use of employee credentials is not permitted under any circumstances.

19.2 Contractors

Contractors making changes to the Firm's network must 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.

19.3 Remote Access

Remote Access to the Firm's networks are governed by the Remote Access policy.

19.4 Enforcement

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

CONFIDENTIALITY AGREEMENT

It is the policy and practice of ToGGeL (hereinafter "the Firm") that the confidentiality of all clients, businesses and related matters are always guarded and protected in every possible and reasonable manner. For that reason, you are being asked in your capacity as an employee or representative of _____ a service provider to the Firm, 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 all other office matters that you may learn in the course of your work with the Firm.

Any breach of this confidentiality policy to third parties will result in the immediate termination of our business relationship. Furthermore, should you breach this confidentiality policy in any way, you and your company will be jointly and severally liable for all damages and expenses incurred.

I, _____, an employee and authorised representative of the abovementioned service provider have read, understood and agree to abide by the provisions of the confidentiality policy.

Signed at _____ on this ____day of _____ 20___.

_____ _____

Signature Print name and surname