1. PURPOSE

1.1. The purpose of the Acceptable Use Policy is to establish the acceptable use of information assets and computer equipment at WTI / EFW Holdings Limited and each of its subsidiaries ("**WTI**"). Inappropriate use exposes WTI to risks including virus attacks, compromise of network systems and services, and legal issues.

2. SCOPE

2.1. This policy applies to the use of information, electronic and computing devices, and network resources to conduct WTI business or interact with internal networks and business systems, whether owned or leased by WTI, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at WTI and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with WTI policies, standards, UK laws and regulations.

3. REFERENCES

Document Number	Title
IT-POL-001	Information Security Policy
IT-POL-003	Acceptable Use Policy
IT-POL-006	Password Policy

4. DEFINITIONS

Term	Definition
User	The collective term used to describe all those who have access to WTI's information and information systems as outlined in the Scope of this policy.
Privileged User	A Privileged User is a user who has an elevated level of access to a network, computer system or application and is authorised to perform functions that standard Users are not authorised to perform. This includes a "standard user" with approved elevated Privileges that allows equivalent access to that of a Privileged User.
PI	Protected Information - includes all forms of sensitive, confidential and proprietary business information, and personal privacy and personal financial information such as that contained in background verifications, employee records, customer records, customer payment/cardholder information, consumer reports, financial, protected health, video records, photographs and certain other types of personal information.
RSS	"Really Simple Syndication"- is a web feed which allows users and applications to access updates to websites in a standardized, computer-readable format. It is used by computer programs that organize those headlines and notices for easy reading. These feeds can, for example, allow a user to keep track of many different websites in a single news aggregator.

5. RESPONSIBILITIES

5.1. Change Configuration Review Board

5.1.1. Members of the Board shall ensure that the necessary controls are implemented and complied with as per this policy.

5.2. IT Manager

5.2.1. Establish and revise the information technology strategy, policy and standards for change management and control with input from interest groups and subsidiaries;

5.2.2. Facilitate and co-ordinate the necessary counter measures to change management and control initiatives and evaluate such policies and standards;

5.2.3. Establish the security requirements for change management and control directives and approval of the change management and control standards and change control/ version control products;

5.2.4. Co-ordinate the overall communication and awareness strategy for change management;

5.2.5. Acts as the management champion for change management and control;

5.2.6. Provide technical input to the service requirements and co-ordinate affected changes to SLA's where applicable.

5.2.7. Establish and co-ordinate appropriate interest group forums to represent, feedback, implement and monitor change management and control initiatives;

5.2.8. Ensure that all application owners are aware of the applicable policies, standards, procedures and guidelines for change management and control;

5.2.9. Co-ordinate the implementation of new or additional security controls for change management; and

5.2.10. Approve and authorise change management and control measures on behalf of WTI.

5.3. IT Service Provider

5.3.1. Shall comply with all change management and control statements of this policy.

5.4. Solution Owners

5.4.1. Shall comply with all information security policies, standards and procedures for change management and control; and

5.4.2. Report all deviations.

6. POLICY

6.1. GENERAL USE AND OWNERSHIP

6.1.1. The WTI may provide computers, computer files, email, telephones, a voicemail system, internet access, software, networks, and other IT Systems to Users for business purposes. In addition, WTI may provide Users with mobile devices through which text messages and other communications are sent and received. These systems, including the information therein, are the property of WTI and are intended for WTI work-related use.

6.1.2. Users are responsible for exercising good judgment when using or accessing IT resources, corporate electronic devices, information assets, and sensitive information.

6.1.3. Under no circumstances shall any User disclose, transmit, or allow access to any information asset to a third-party without authorization.

6.1.4. Under no circumstances shall any User allow an IT resource to be accessed or used by a third-party without authorization.

6.2. ACCEPTABLE USE OF IT SYSTEMS

6.2.1. While WTI does not prohibit or prevent Users from using IT resources for personal use, WTI expects that such personal use will not diminish in any significant way the use of these systems by others engaged in WTI's business, or interfere with any User work-related activities or performance, or compromise the security of WTI's network.

6.2.2. Users should never disclose Protected Information to anyone directly or in response to any email where they cannot trust the source of the email or communication and should refer to IT Support if they receive a suspicious communication.

6.2.3. IT resources and corporate devices are the property of WTI and therefore Users should understand that certain activities may be monitored for security purposes. For example, WTI email may be read and/or monitored as required. WTI has the right to copy, examine, or disclose any or all email messages and information accessed or processed by, stored on, or communicated using WTI IT resources.

6.2.4. All devices connected to the WTI network must continually execute WTI mandated security components. Users shall not disable or modify any security components on any IT resources unless specifically authorized to do so.

6.2.5. In the event that any User is made aware of inappropriate use of the systems, including information security violations or the possible introduction of a virus, the **IT Manager** should be notified immediately. If a User is confident that the source of the communication is legitimate, he or she should still consider using appropriate mechanisms to share information, including encryption, password protected files and only sharing necessary information. Further

guidance on sharing personal data can be found in the Electronic Personal Data Transmission Policy.

6.3. COMPANY'S RIGHT TO ACCESS SYSTEMS AND INFORMATION

6.3.1. The WTI's IT Systems are WTI's property, and employees do not have a personal privacy right in any matter received, sent or maintained on these systems. To ensure compliance with this policy, computer, internet, mobile device, text message and email usage may be monitored by WTI.

6.3.2. WTI has the right to access and monitor information and may conduct unannounced inspections of WTI IT Systems in accordance with applicable law. Email, voicemail, text messaging and Internet access are IT Systems provided by WTI primarily to enable employees to send and receive business information rapidly and efficiently.

6.3.3. Excessive use of any electronic communication for non-business purposes will result in disciplinary action up to and including termination of employment.

6.4. COMPANY MOBILE DEVICE USE

6.4.1. The company will, at its discretion and in accordance with this policy, provide employees with mobile devices and telecom carrier services, at WTI's expense, for the primary purpose of conducting WTI business. All mobile devices provided by WTI are the property of WTI and the employee is responsible for ensuring the appropriate use of the mobile device, as well as the security and safe keeping of the mobile device as outlined in this Policy.

6.4.2. MIFIs are devices that facilitate wireless connectivity for laptop computers through a company approved wireless carrier's network. WTI allows the use of MIFIs on a limited basis for Users, depending upon need (travel, etc.). The IT Department maintains a small inventory of MIFI devices for UK Users, who can request a loan MIFI by submitting a Helpdesk ticket.

6.4.3. Approved mobile devices (whether WTI or User-owned) may be configured to send and receive WTI email. WTI or User-owned mobile devices should not be configured to back up or sync WTI email to any type of cloud service (e.g. Google Cloud, Apple iCloud, etc.).

6.4.4. Mobile device usage will be monitored on a monthly basis, including reviewing data consumption & trend analysis reports at the individual level. The WTI's existing plan allows for unlimited voice and text usage, along with a shared data pool adequate for WTI's business needs. Users are reminded that streaming non-work-related movies, videos, or music is not allowed.

6.4.5. The safety of WTI Users is critical to our ongoing success. Therefore, WTI prefers that mobiles are not used when driving. If calls are

absolutely necessary WTI requires all Users with a WTI-owned mobile device to utilize handsfree equipment when using the mobile device while operating a WTI owned vehicle, personal vehicle, or rental vehicle for business.

a) Only voice calls with hands-free equipment is permitted. When dialling a number, employees should pull over to the side of the road in a safe location or use voice activated calling or preprogramed numbers providing it does not distract from safe driving. Any other mobile device-enabled activity that prevents a User from focusing on driving such as surfing the internet, text messaging, checking email, the use of applications or other activities, is prohibited.

b) The WTI requires its employees to adhere to all UK laws and regulations regarding the use of mobile devices while operating a motor vehicle. For more information on the specific laws and regulations in the UK, access this link.

6.5. USE OF PERSONAL DEVICES AND SYSTEMS

6.5.1. Supervisors may request that IT provide certain key employees with the ability to receive WTI email on personal mobile devices, however, those devices shall be subject to password policies and other restrictions in order to protect WTI's data in the event the device is lost or stolen. If such access is provided, it will thereafter be the User's responsibility to notify IT on a timely basis if those personal mobile devices are lost, stolen, discarded, upgraded, replaced or otherwise no longer required for those purposes, so the devices can be properly wiped of WTI email and other data, and the ability to sync with WTI's email servers can be removed.

6.5.2. User-owned mobile devices will be subject to encryption and any other security policies and practices deemed necessary by WTI to ensure the security of WTI data, including remote wipe upon termination. User-owned mobile devices may not connect to WTI's internal network.

6.5.3. Users should be aware that any external communication via e-mail that is delivered over the internet is not encrypted and may be intercepted, copied, and/or modified during transmission by a third party. As such, users must not transmit any Protected Information over the e-mail system if it utilises the Internet for delivery to the recipient without specific arrangements to secure and encrypt the contents of the message.

6.5.4. Users should understand that e-mail, text messages and voicemail messages may have to be disclosed in lawsuits, and sometimes to people and entities with interests adverse to WTI's interests. Accordingly, Users should use their best judgment in sending or responding to e-mail or text messages, or in leaving a voicemail message.

6.5.5. Users are prohibited from storing Protected Information on portable devices or media (laptop, external disk drive, smart phone, tablet, USB drive, CD/DVD, etc.) unless that device or media has been configured with a WTI-approved encryption solution.

6.5.6. All Protected Information in paper form must be stored within restricted access, secure (e.g. under lock and key) facilities, storage areas, or containers.

6.5.7. WTI information should not regularly be stored on the hard disk drive or other internal components of a personal computer. Information must be stored on network drives or in WTI's cloud storage to ensure that regular backups of the data occur. In instances where temporary storage of WTI information on the hard disk of a WTI laptop is necessary, the files must be encrypted.

6.6. SECURITY OF IT SYSTEMS

6.6.1. Users must ensure that use of WTI's IT Systems, especially those involving Internet access and access to Protected Information, does not compromise the security of WTI's computer systems and networks or risk disclosure of Protected Information. These duties include taking reasonable precautions to prevent intruders from accessing WTI's network (e.g., logging off of the network and securing your laptop before leaving the office, and following all password and User authentication protocols).

6.6.2. All material received on disk or other magnetic or optical medium and all material downloaded from computers and networks not belonging to WTI must be scanned for viruses and other destructive programs before being placed on WTI IT Systems. In addition, because personal media or equipment may contain viruses, personal media or equipment should never be brought to a WTI site and connected to WTI IT Systems or networks.

6.7. PROHIBITED USE

Users are prohibited from:

6.7.1. Using WTI's IT systems in any way that may be disruptive, offensive or harmful to others, including, but not limited to, accessing websites, or downloading, displaying or transmitting cartoons, gossip, profanity, defamation, vulgarity, sexual content or any other material that would violate WTI's policies or be construed as offensive, harassing or disrespectful to a reasonable person (for example, a racial or ethnic slur, sexual comments or images);

6.7.2. Using WTI's IT systems to display material that may incite or encourage others to carry out unauthorized access to or modification of computer systems, networks or data);

6.7.3. Using or encouraging others to use WTI's IT voice or data systems or networks to disseminate or access materials of an illegal, obscene, pornographic, or excessively violent nature or to otherwise misuse or tap these systems;

6.7.4. Using WTI's IT systems to display or disseminate material that discriminates or encourages discrimination on the grounds of gender, sexual orientation, race or ethnic origin;

6.7.5. Using WTI's IT systems for solicitation of non-WTI related business, selling non-WTI related products or otherwise engaging in non-WTI related commercial activities other than those expressly permitted by WTI management;

6.7.6. Use of WTI's IT systems that taxes the system's bandwidth and speed such as installing or downloading software to WTI equipment (e.g., MP3 or file sharing programs), signing up for RSS feeds, or streaming music, podcasts, or HD video content that is non-business-related;

6.7.7. Using or disclosing another User's code or password and from accessing any email or voicemail other than their own unless express permission has been given, in writing, from the IT Manager. If an employee is granted such access, the employee must follow the same obligations as set forth in this policy, as if the messages were his or her own;

6.7.8. The unauthorized use of IT assets, including installing new hardware/software without permission from the IT Department, printing, copying or distribution of copyrighted, trademarked, or patented material;

6.7.9. Sharing access passwords and User authentication protocols with others. Users are accountable for the use of such passwords, and are expected to keep passwords confidential;

6.7.10. Using WTI communication resources for personal gain or entertainment (e.g., sending chain letters);

6.7.11. Forwarding email that either originates from an external mail system (e.g. Gmail, Yahoo, Hotmail, etc.) to WTI's email system, OR from WTI's email system to any external system;

6.7.12. Using software on local area networks or on multiple machines in violation of the relevant software license agreement.

6.8. MEDIA GUIDELINES

6.8.1. Every User is responsible for ensuring the physical security of all media containing Information Assets under their control and accountable for any loss of any WTI corporate device.

6.8.2. Electronic Media (such as backup tapes, videos, voice recordings, photographs) bound for offsite storage must be encrypted before being placed in transit.

6.8.3. Electronic data written to CDs/DVDs/external hard drives or other similar media shall be labelled appropriately and stored in a locked, restricted-access cabinet or room at WTI facilities.

6.8.4. Paper documents containing confidential information should not be left unattended. They should be protected from the view of passers-by, office visitors, cleaning crews, etc.

6.8.5. Paper documents should be stored in locked files. Keys to file drawers should not be left in unlocked desk drawers or other areas accessible to unauthorized personnel.

6.8.6. Documents that are printed on copy machines, fax machines and printers should be immediately retrieved or secured, or printed directly to a limited-access mailbox, where possible.

6.9. CLEAN DESK GUIDELINES

6.9.1. WTI utilizes processes to establish the minimum requirements for maintaining a clean desk and keeping Protected Information Secure.

6.9.2. Users are required to ensure that all Protected Information in hardcopy or electronic form is locked away when the User is expected to leave the desk for an extended period. If electronic Protected information is on a computer, the User must log off, sign-out, or lock the screen when leaving the computer unattended.

6.9.3. Computer workstations must be shut completely down at the end of the workday.

6.9.4. Protected Information must be removed from the desk and locked in a drawer when the desk is unoccupied at the end of the working day.

6.9.5. File cabinets containing Protected Information or must be kept closed and locked when not in use or when unattended.

6.9.6. Keys used for access to Protected Information must not be left at an unattended desk.

6.9.7. Laptops, tablets, and all portable computing devices must be locked away in a drawer or an office when not in use.

6.9.8. Passwords should be kept private and all Users should refrain from keeping an unsecured record of their password, e.g. by storing it on sticky note or under a computer.

6.9.9. Printouts containing Protected Information should be removed immediately from printers, fax, machines and not left unattended in public areas.

6.9.10. Protected Information should be disposed of using an office document shredder or placed in a locked confidential disposal bin.

6.9.11. Whiteboards with Protected Information must be erased.

6.10. TROUBLESHOOTING

6.10.1. Should any IT resource require troubleshooting or service of any kind, Users shall only permit authorized WTI IT Support to perform such troubleshooting or service unless directed otherwise by the IT Manager. Under no circumstances shall a User independently allow an unauthorized third-party access to IT resources for the purposes of troubleshooting or performing service on that IT resource.

6.11. SOFTWARE INSTALLATION

6.11.1. To minimize the risk of loss of program functionality, the exposure of Protected Information contained within WTI's computing network, the risk of introducing malware, and the legal exposure of running unlicensed software, Users shall not be provided with administrative rights to WTI-owned computing devices unless an exception is granted by the IT Manager.

6.11.2. Users may not install software on WTI-owned computing devices operating within WTI network without the prior authorization of the IT Manager. The use of unapproved software on IT resources may be terminated and the software removed at any time by WTI should its continued use pose an unacceptable risk to the integrity and security of WTI's IT systems. Such software may also be removed upon evidence of misuse or interference with the proper operation of the IT resource.

6.11.3. Software requests must first be approved by the requester's manager and then a ticket shall be opened and approved by the IT Manager. IT will obtain and track the licenses and perform the installation.

6.12. REMOTE ACCESS AND TELEWORKING

6.12.1. All Users working from a non-WTI location using remote access and teleworking access shall ensure the following:

c) Users will only use WTI-managed corporate devices when connecting to WTI network.

d) Users will connect using secure communication mechanisms (i.e. Virtual Private Network (VPN) connection).

e) WTI IT resources will only be backed up to encrypted drives owned and provided by WTI. Under no circumstances will IT resources be backed up to any personally owned backup system, or device, or cloud service.

6.13. WIRELESS NETWORK ACCEPTABLE USE

6.13.1. While wireless networks are exposed to many of the same risks as wired networks, they are vulnerable to additional risks as well. Wireless networks transmit data through radio frequencies and are open to

intruders unless protected. Intruders can exploit this openness to access systems, destroy or steal data, and launch attacks that tie up network bandwidth and deny service to authorized Users. Protecting the network from such intrusions is a shared responsibility among users and IT.

6.13.2. Users of WTI wireless network must comply with all WTI policies applicable to the wired network. The following is prohibited:

a) Using a wireless enabled device or wireless access point to provide access to WTI wireless network, wired network, or the Internet to Users who are not approved for such access.

b) Using a wireless enabled device or wireless access point to extend WTI-approved coverage areas of WTI's wireless network infrastructure.

c) Sharing the password for WTI wireless network access with unauthorized personnel.

6.14. NETWORK AND EMAIL STORAGE

6.14.1. All WTI files and messages must be stored in WTI file shares or cloud services.

6.14.2. **Personal File Shares.** A personal file share is created for each employee as part of the new User set up process. This storage area is available for individual use and cannot be shared with others. Each User has control over his/her files in this space, including the ability to create, update/edit and delete files. This is the best place to draft and store documents prior to their finalization:

a) Suggested uses include:

i. Active file storage for individuals

ii. Draft documents prior finalization

iii. Convenience copies of confidential documents (e.g. employee performance review)

b) Not intended for:

i. Active file storage for departments

ii. Administrative information storage

iii. Critical departmental documents and records or customer correspondence

iv. Departmental file sharing

v. Inter-departmental file sharing

vi. Nonwork-related movies, music, pictures, etc.

6.14.3. **Departmental File Shares.** Departmental file shares have been created for all corporate departments (Finance, Legal, Commercial, etc.) and plants. Files in this storage space are shared among those who have been identified as members of each department or group. The “owner” (typically a department head or Plant Manager) of a departmental share determines who has access to all the files in the share as well as what type of access. The access type options are "read-only," or "read, write, modify”.

a) Suggested use:

i. Active file storage for departments

ii. Administrative information storage

iii. Critical departmental documents, and records, customer correspondence, etc.

iv. Departmental file sharing

b) Not intended for:

i. Active file storage for individuals

ii. Personal document archival

iii. Inter-departmental file sharing

iv. Nonwork-related movies, music, pictures, etc.

6.14.4. **Inter-Departmental File Shares.** Inter-departmental file shares are available upon request to facilitate inter-departmental file sharing. Access and control is managed in a way similar to Departmental File shares.

a) Suggested Uses

i. Active file storage for groups

ii. Administrative information storage

iii. Critical inter-departmental document archival

iv. Inter-departmental file sharing

b) Not Intended for:

i. Active file storage for individuals

ii. Personal document archival

iii. Departmental file sharing

iv. Nonwork-related movies, music, pictures, etc

6.14.5. **Email Storage**: Messages and Attachments.

a) WTI’s Email servers comprise a critical messaging and communication system for Users. The system is not intended for long-term storage of email and attachments, except as detailed below.

b) In general, messages and attachments should be deleted if no longer needed, or permanently stored on a WTI file server, to ensure that available disk space is managed and to ensure the reliability and availability of WTI's data and computing resources. When Users store important messages and attachments indefinitely in the email system, they are not readily available to anyone else in WTI. If properly stored electronically on a file server, they are readily available to others with similar permissions and they remain readily available even as Users retire or otherwise leave WTI. As such, important WTI records belong on the file server in departmental folders, not in individual mailboxes. If an employee is unsure as to where or whether an email message or attachment should be stored, he or she should check with their supervisor, WTI's General Counsel, or refer to WTI's Records Management Procedure.

6.14.6. **Email Accounts**. An email account is created for most Users as part of the new User set up process. This account is available for individual use and cannot be shared with others. Each User has full control over his/her email, including the ability to create, send, receive, store, and delete messages and attachments. All mailboxes are subject to quotas which Users must manage within.

6.14.7. Records and Email Management Policies. WTI records can include files, email, pictures, recordings and many other types of records in both paper and electronic form. Records Management Policies support several objectives:

a) Ensuring the proper classification and protection of important WTI records.

b) Requiring regular deletion of non-essential and/or duplicative files and/or email from WTI resources.

c) Providing guidelines relevant to data associated with a "Legal Hold".

d) Enabling prudent utilization and conservation of WTI resources, such as disk storage and Exchange/Outlook.

6.14.8. **Email Management Strategies.** Managing your mailbox can be simplified if you frequently send or receive large files to/from the same groups:

a) Large, internally created files which are distributed regularly and frequently (e.g. a daily report) can often be distributed to other internal parties by sending a document link, rather than the document itself. Please contact the IT Department for assistance with access permissions and link creation.

b) Large, externally created files which are received regularly and frequently (e.g. a daily report) can be distributed to internal parties by requesting a group email address and automated process created for this purpose. Please contact the IT Department for

more information about this alternative.

6.15. POLICY ENFORCEMENT

6.15.1. All Users are responsible for understanding and abiding by IT policies set forth by WTI.

6.15.2. Users who discover violations of this policy or deficiencies in the security of WTI's IT Systems should notify the IT Manager, HR Director, or other member of management.

6.15.3. Failure to comply this policy may be subject to disciplinary action, up to and including termination of employment. A User's computing privileges may be suspended or restricted during the investigation of a problem.

6.15.4. Immediately upon termination of employment or of a contractual relationship, Users are prohibited from accessing WTI IT Systems and shall be required to return all WTI-issued equipment without delay.

7. IMPLEMENTATION

The UK Chief Financial Officer is responsible for the implementation of this Policy and other related policies and procedures, including the communication and detailed interpretation, monitoring and any disciplinary action in response to an apparent breach of this Policy. The UK IT Manager is responsible for maintaining and reviewing this Policy and for clarifying and resolving any issues arising in relation to it.

8. REVISION HISTORY

Revision	Issue Date	Approval Date	Summary of changes	Approved by:	Next Review
1.0	06/10/20	21/10/20	Initial Release	IT Manager	06/10/21