Frontera Consulting Information Security Policy

The **Frontera Consulting Information Security Policy** (the "**IS Policy**") promotes an effective balance between information security practices and business needs. The IS Policy helps Frontera Consulting LLC, Frontera Consulting Ltd. And Frontera Consulting HK Limited (collectively, the "Company") meet its legal obligations in the countries from which it conducts its operations, and our clients' expectations. All provisions of this IS Policy are subject to the laws in the country in which you are based and apply to the extent permitted by those laws. This IS Policy applies to your use of all the Company's information equipment including all systems, hardware, software, data, databases, telecommunications links and equipment, content and other materials (together the "IT Systems") the Company makes available to you. This IS Policy also applies to any clients of the Company and to the information equipment including all systems, hardware, software, data, databases, telecommunications links and equipment, content and other materials (together the "IT Systems") our clients make available to you. From time to time, the Company may implement different levels of security controls for different information assets, based on risk and other considerations.

You are expected to read, understand, and follow this IS Policy. However, no single policy can cover all the possible information security issues you may face. You must seek guidance from your manager or other Company resource before taking any actions that create information security risks or otherwise deviating from this IS Policy's requirements. The Company may treat any failure to seek and follow such guidance as a violation of this IS Policy.

This IS Policy is Confidential Information. Do not share this IS Policy outside the Company unless authorized by the Information Security Coordinator. You may share this IS Policy with an approved contractor that has access to the Company's information or systems under a non-disclosure agreement or other agreement that addresses confidentiality.

Our clients, employees, and others rely on us to protect their information. An information security breach could severely damage our credibility. Security events can also cause loss of business and other harm to the Company. Strong information security requires diligence by all workforce members, including employees, contractors, volunteers, and any others accessing or using our information assets. It is part of everyone's job.

1. Purpose and Scope

1.1. The Company aims to provide the highest standard of service to its clients and employees. In order to achieve a consistently high level of professional service, it is vital that the Company's IT Systems are fully operational at all times. Security, in particular computer security, is of paramount importance, as much of staff and clients' confidential information is stored in the Company's databases.

1.2. Moreover, the internet, e-mail and in many cases instant messaging and other technologies are integral parts of the typical employee's daily routine. Alongside the growing business dependency on the use of new communications technologies, a number of employee-related problems may arise. One such problem is the downtime associated with employees sending and receiving personal communications or recreationally surfing the internet.

1.3. This can have an enormous impact on an organization of our size both on productivity and profitability. It is our aim to ensure that the Company's IT Systems are used responsibly and safely by all but not to the detriment of the Company. Internet and email abuse can have very damaging effects on a company's reputation.

1.4. This IS Policy sets out the procedures and guidelines relating to the correct use of computerized systems within the Company and explains how it can be achieved. The purpose of the IS Policy is to ensure that an effective and high standard of service is provided to the Company's clients and to you through compliance with this IS Policy and that best practice and any applicable legislation are complied with.

In many cases, you are personally responsible for taking or avoiding specific actions as the IS Policy states. In some situations, Human Resources, or another Company resource takes or avoids the stated actions.

1.5. This IS Policy provides detailed information security guidance that you must follow in addition to any obligations listed in our CODE OF CONDUCT. From time to time, the Company may approve and make available more detailed or location or business unit-specific policies, procedures, standards, and processes to address specific information security issues. Those additional policies, procedures, standards, and processes are extensions to this IS Policy. You must comply with them, where applicable, unless you obtain and approved exception. The Company may treat any attempt to bypass or circumvent security controls as a violation of this IS Policy. For example, sharing passwords, deactivating anti-virus software, removing or modifying secure configurations, or creating unauthorized network connections are prohibited unless the Information Security Coordinator has granted an exception as described in this IS Policy.

1.6. If you have any questions about this IS Policy, or if anything is unclear, please contact HR, for practice-related queries regarding the use of IS.

1.7. On at least an annual basis, the Information Security Coordinator will initiate a review of this IS Policy, engaging stakeholders such as individual business units. Human Resources, Legal and other Company organizations, as appropriate.

1.8. The Company recognizes that specific business needs and local situations may occasionally call for an exception to this IS Policy. Exception requests must be made in writing. The Information Security Coordinator must approve in writing, document, and periodically review all exceptions. Do not assume that the Information Security Coordinator will approve an exception simply because he or she has previously approved a similar exception. Each non-compliant situation requires a review of the specific facts and risks to the Company's information assets and those of our clients. To request an exception, contact HR.

2. Guiding Principles

2.1. The Company follows the following guiding principles when developing and implementing information security controls:

2.1.1. The Company strives to protect the confidentiality, integrity, and availability of its information assets and those of its clients.
2.1.2. We will comply with applicable privacy and data protection laws.
2.1.3. We will balance the need for business efficiency with the need to protect sensitive, proprietary, or other confidential information from undue risk.
2.1.4. We will grant access to sensitive, proprietary, or other confidential information only to those with a need to know and at the least level of privilege necessary to perform their assigned functions.
2.1.5. Recognizing that an astute workforce is the best line of defense, we will provide security training opportunities and expert resources to help individuals understand and meet their information security obligations.]

3. Acceptable Use

3.1. The Company's IT systems are provided to enable you to perform your duties as an employee of the Company. Usage of these systems is primarily for work-related purposes. However, the Company recognizes that employees on occasion may need to make some personal use of the IT Systems. You should not however use the Company's resources for commercial purposes, personal gain, or any purpose that may create a real or perceived conflict of interest with the Company.

3.2. You are permitted to make limited reasonable personal use of the IT Systems, providing your usage complies with this IS Policy, has no negative impact on the Company, does not incur any significant expenses nor take a significant amount of time and has no adverse impact on carrying out your job or that of your colleagues. Except in exceptional circumstances, any personal use of the Company's network and IT Systems should be restricted to the following times: - before the start of the working day, at break times and at the end of the working day only. The assessment of excessive use will be at the sole discretion of management. Personal telephone calls should be kept to a minimum and only made or taken when necessary. The Company's network and IT Systems are subject to monitoring (See Section 7, Privacy and Monitoring].

3.3. Furthermore, all employees must behave in a proper, ethical and legal manner consistent with all Company policies (including this policy) when using the Company's IT Systems both for business and personal purposes. In particular you must not, without limitation, use them:

3.3.1. in any way that may be deemed unlawful, illegal, abusive or fraudulent under applicable federal, state, local, or international law; if the Company suspects illegal activities, it may report them to the appropriate authorities and aid in any investigation or prosecution of the individuals involved
3.3.2. to send or promote the sending of any unsolicited, unauthorized mass distributed advertising or unauthorized promotional material;
3.3.3. to sell any goods which require a license;
3.3.4. in any way which infringes the Company's Intellectual Property Rights;
3.3.5. in any way which breaches your obligations of confidentiality to the Company or the Company's confidentiality to its clients;
3.3.6. for online gambling or contribution to internet discussion groups;
3.3.7. to engage in hacking, spoofing, or launch denial of service attacks;
3.3.8. to gain or attempt to gain unauthorized access to others' networks or systems;
3.3.9. to send fraudulent email messages;
3.3.10. to distribute or attempt to distribute malicious software (malware);
3.3.11. to spy or attempt to install spyware or other unauthorized monitoring or surveillance tools;
3.3.12. to commit criminal acts such as terrorism, fraud, or identity theft;
3.3.13. to download, store, or distribute child pornography or other obscene materials;
3.3.14. to download, store, or distribute materials in violation of another's copyright;
3.3.15. to create undue security risks or negatively impact the performance of the Company's network and IT Systems;
3.3.16. to cause embarrassment, loss of reputation, or other harm to the Company;
3.3.17. to upload, download, or disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, threatening, obscene, or otherwise inappropriate or offensive messages or media;
3.3.18. to distribute joke, chain letter, commercial solicitations, or hoax emails or other messages (spamming);
3.3.19. to disrupt the workplace environment, create a hostile workplace, or invade the privacy of others;
3.3.20. to use encryption or other technologies in an attempt to hide illegal, unethical, or otherwise inappropriate activities; and
3.3.21. to install or distribute unlicensed or pirated software.

3.4. You must not install, load, access or otherwise use any software or device on any part of the Company's IT Systems unless specifically authorized in writing by Group IT. You must not use or install any unlicensed software on the Company's IT Systems in any circumstances. Any files or software downloaded from the Internet or brought from outside the Company must be virus checked before use. You must not run any '.exe'. files. These should be deleted immediately upon receipt without being opened. You may be denied remote access using non-Company owned or approved devices that do not meet the Company's then-current minimum information security standards.

3.5. Use your own Company-provided account(s) to access the Company's network and IS Systems, unless you have been specifically authorized to use a device-specific, administrative, or other account (see Section 11.2, Identity and Access Management). You must not install any passwords (except your own personal password) which restrict or limit access to the systems or any part of them. Screen saver passwords, also known as "workstation timeouts" or "lock screens", secure Confidential Information by protecting active computer sessions when you step away. Locking screen savers must activate after a maximum inactivity time of 15 minutes. If you handle Highly Confidential Information, lock your screen any time you leave it unattended.

3.6. You must properly handle, store, and securely dispose of the Company's information in accordance with the Company's Data Retention Schedule. You are responsible for any Confidential or Highly Confidential Information that you access or store. Do not allow others to view, access, or otherwise use any Confidential or Highly Confidential Information you control unless they have a specific business need to know.

Store files or other data critical to the Company's operations on regularly maintained (backed up) servers or other storage resources. Do not store business critical data only on end-user devices such as desktops, laptops, smartphones, or other mobile devices.

Physically secure any media containing the Company's information, including hard drives, CDs, disks, paper, voice recordings, removable drives (such as thumb drives, flash drives, USB drives), or other media. Media containing Confidential or Highly Confidential Information must be stored in a locked area when not in use.

Shred or otherwise destroy paper that contains Confidential or Highly Confidential Information prior to disposal. Return all electronic, magnetic, or optical media Group IT for secure disposal when it is no longer required to meet business needs.

3.7. Internet Use: Email, Messaging, Social Media, and Cloud Computing. The internet offers a variety of services that the Company's employees [and contractors] depend on to work effectively. However, some technologies create undue risks to the Company's assets. Some uses are not appropriate in the workplace.

The Company may block or limit access to particular services, websites, or other internet-based functions according to risks and business value. Recognize that inappropriate or offensive websites may still be reachable and do not access them using the Company's resources.

3.7.1. General Internet Use. Limit your web browsing and access to streaming media (such as videos, audio streams or recordings, and webcasts) to business purposes or as otherwise permitted by this IS Policy. Internet use must comply with this Policy.

Never use internet peer-to-peer file sharing services, given the risks to the Company's information assets they create.

Do not use internet-based remote access services to access the Company's network or IT systems, including desktop computers. If you need remote access, use the Company-provided or authorized software (see Section 3.9, Remote Access).

3.7.2. Email and Social Media. Do not disclose Confidential or Highly Confidential Information to unauthorized parties on blogs or social media or transmit it in unsecured emails or instant messages (see Section 10, Data: Information Classification and Risk-Based Controls). Do not make postings or send messages that speak for the Company or imply that you speak for the Company unless you have been authorized to do so.

Use good professional judgment when drafting and sending any communications. Remember that messages may be forwarded or distributed outside your control, and your professional reputation is at stake. Email signatures should be professional, appropriate for your business role, and not unreasonably long or complex. [The Company provides standard email footer text that must be placed on all externally bound email messages. Do not alter or prevent application of the standard footer to your external messages.]

Never open an email attachment that you did not expect to receive, click on links, or otherwise interact with unexpected email content. Attackers frequently use these methods to transport viruses and other malware. Be cautious, even if messages appear to come from someone you know, since attackers can easily falsify (spoof) email senders. The Company may block some attachments or emails, based on risk.

Do not respond to an email or other message that requests Confidential or Highly Confidential Information unless you have separately verified and are certain of its origin and purpose. Even then, always protect Confidential or Highly Confidential Information as described in Section 10, Data: Information Classification and Risk-Based Controls.

If you have any doubts regarding the authenticity or risks associated with an email or other message you receive, contact Group IT immediately and before interacting with the message. Do not reply to suspicious messages, including clicking links or making unsubscribe requests. Taking those actions may simply validate your address and lead to more unwanted or risky messages.

3.7.3. Cloud Computing. The Company may use internet-based, outsourced services for some computing and data storage activities based on business needs. Cloud computing services store data and provide services in internet-accessible data centers that may be located almost anywhere. Cloud services vary significantly in-service levels and security provided.

While cloud services may offer an attractive cost model, they also present significant risks. Using them may also affect the Company's ability to comply with some laws. Before using any cloud computing services to collect, create, store, or otherwise manage the Company’s Confidential or Highly Confidential Information, you must obtain approval from Legal and the Information Security Coordinator (see Section 13, Service Providers: Risk and Governance).

This IS Policy applies to any document sharing or other internet-based services, if Company Confidential or Highly Confidential Information is stored.

3.8. Mobile Devices and Bring Your Own Device to Work. Mobile devices, including laptops, smartphones, and tablet computers, can provide substantial productivity benefits. Mobile storage devices may simplify information exchange and support business needs. However, all these mobile devices also present significant risks to the Company's information assets, so you must take appropriate steps to protect them.

The Company may permit employees and others to use their own equipment to connect to its network and systems. If you choose to do so, you agree that your use of those devices is subject to this IS Policy and any additional policies, procedures, standards, and processes the Company implements. You may be required to install specific security controls on your device (for example, device management software, access controls, encryption, remote wiping in case your device is lost or stolen, or other security controls).

You must allow Group IT to review your device and remove any Company data, if your relationship with the Company terminates, you change devices or services, or in other similar situations. You must also promptly provide the Company with access to your device when requested for the Company's legitimate business purposes, including any security incident or investigation.

Use encryption, other protection strategies (for example, device management software, access controls, remote wiping in case your device is lost or stolen, or other security controls), or both on any mobile device that contains Confidential or Highly Confidential Information. Mobile devices, including those that provide access to Company email, must be protected using a password or other approved authentication method.

Physically secure any mobile devices you use to access or store Company information. Never leave laptops or other devices unattended unless locked or otherwise secured. Do not leave mobile devices or the bags containing them visible in a parked car or check them as baggage on airlines or other public transportation.

Do not connect a mobile device containing Company information to any unsecured network without an up-to-date firewall configured (or other security controls in place). Unsecured networks include home networks, hotel networks, open or for-pay wireless hotspots, convention networks, or any other network that Company has not approved or does not control.

3.9. Remote Access. If you have a business need to access the Company's network and systems fromhome, while traveling, or at another location, the Company may grant you remote access.

Use two-factor authentication to access the Company's network remotely. Configure remote access capabilities to limit access to only those assets and functions the Information Security Coordinator approves. You may only use Company-provided means for remote access (for example, VPN connections, dial-up modems, the Company’s portal). Do not install or setup any other remote connections, including remote desktop software, without the Information Security Coordinator's authorization.

Remote access connections should timeout (be disconnected) after a maximum of one hour of inactivity. The Company does not permit split tunneling or other mechanisms that bridge unsecure networks with the Company's network.

3.10. External Network Connections. Some business situations may require creating a secure connection from the Company's network to an external party's network (extranet). Examples include working extensively with client systems, outsourcing, or partnering with another organization for an extended period of time. Extranet connections allow the organizations to share information and technical resources in a secure manner by connecting the two networks at their respective perimeters.

The Information Security Coordinator must review and approve all extranets and any other external connections the Company's network before implementation. A signed business agreement between the two organizations must accompany any extranet connection. Limit connectivity to only those assets required to perform the specified functions. The Company monitors extranet connections and may deactivate them if unusual or inappropriate traffic is detected.

3.11. Wireless Network Connections. Do not connect any wireless access points, routers, or other similar devices to the Company's network unless the Information Security Coordinator has reviewed and approved them.

Secure and maintain approved wireless network (WiFi) connections according to current Company technical and physical security standards. Do not connect wireless access points (WAPs) directly to the Company's trusted network without going through a firewall or other protective controls. Deactivate WAPs when they are not in use, including during non-business hours.

Only transmit, receive, or make available Highly Confidential Information through WiFi connections using appropriate protective controls, including encryption. If you have questions regarding appropriate WiFi security measures to take when handling Highly Confidential Information, contact the Information Security Coordinator.

End-user devices that access wireless networks, such as laptops, must have personal firewalls installed and maintained according to current Company standards. Deactivate your computer's wireless networking interface when it is not in use.

4. Messages

4.1. Email is a permanent form of written communication, and material can be recovered even when it is deleted from your computer. Emails can give rise to binding obligations and expose the Company to liability in the same way as conventional correspondence. You should not transmit anything in an email that you would not be comfortable writing in a letter or memorandum.

4.2. You must not use the Company's IT Systems to send, receive, forward, access, upload, download, transmit or otherwise deal with material which is abusive, offensive, defamatory, obscene, menacing, indecent, which could constitute bullying or harassment, racist, sexist or otherwise unlawful or illegal, or contains anything of a sexual, violent, political, terrorist or religious nature, or in breach of any copyright, privacy or any other rights. You should also avoid creating email congestion by sending trivial messages or unnecessarily copying emails.

4.3. Automated email forwarding from Fronteraconsulting.net domain is not allowed. No exceptions will be made to this policy.

4.4. If you receive an email containing material that is offensive or inappropriate to the working environment, you must delete it immediately. Under no circumstances should such mail be forwarded either internally or externally.

4.5. Ensure that you make clear that any personal messages are not associated with the Company. This includes ensuring that any personal documents do not use the Company's letterhead, logos or letter stationery.

5. Passwords

5.1. You are responsible for ensuring that your username and password used in connection with the system is kept secure and confidential and is used only by you. You must not allow other employees or any other persons to use your password. You must inform the Company immediately if you know or suspect that your user name or password has been disclosed to anyone else or is being used in an unauthorized way.

6. Data Protection

6.1. Various information security laws, regulations, and industry standards apply to the Company and the personal information we handle. The Company is committed to complying with applicable laws, regulations, and standards. Our clients expect nothing less from us.

6.2. State laws and most countries in the world protect individuals' personal information, such as Social Security numbers, driver's license numbers, financial account information, and other sensitive data. Most states in the U.S. have enacted breach notification laws, and the European Unionis about to enact the same as part of the entry in force of the upcoming General Data Protection Regulation (GDPR) on May 25, 2018. These breach notification laws require organizations to notify affected individuals if personal information is lost or accessed by unauthorized parties. Most states and EU Member States have enacted data protection laws that require organizations to protect personal information using reasonable data security measures or more specific means. These laws may apply to personal information for the Company's employees, clients, business partners, and others.

6.3. Before collecting, creating, or using personal information for any purpose, contact Operations to make sure you understand how we collect and use your and our client's personal information, and that you align your collection and use of that information on our Privacy Policy statements. Personal information about you will be stored and processed by the Company in connection with your contract of employment and for other purposes related to your employment. Storage and processing of your personal information will always be carried out fairly and in accordance with the legislation applicable to your country. Your personal information will only be disclosed to third parties where necessary and will always be done in accordance with local laws.

6.4. This may involve the sharing of data with Group Companies in other countries, some of which may not have the same degree of data protection as your country, in which case such international transfer will be done in accordance with applicable privacy laws. Nevertheless, the Company and all Group Companies will keep your personal data confidential and secure and use it only for purposes and activities related to your employment.

6.5. In certain countries employees are entitled to have access to the information held about them. If you wish to review the personal data held about you by the Company, please contact your manager or HR.

7. Privacy and Monitoring

7.1. Except where applicable law provides otherwise, you should have no expectation of privacy when using the Company's network or systems, including but not limited to, transmitting and storing files, data, and messages.

7.2. The Company reserves the right to monitor any and all use of its network and IT Systems (including emails and shared servers) by employees and contractors, to the extent permitted by local law, for purposes such as ensuring proper operation of its systems, checking compliance with its policies (including this IS Policy), preventing or detecting crime or fraudulent activity, or for other legitimate business purposes. By using the Company's IT systems, you agree to such monitoring.

7.3. The Company reserves the right to use automatic monitoring of web access and email volume to the extent permitted under local laws. This may include the use of software to monitor internet usage including blocking access to inappropriate sites, and software used to monitor the content of emails and to block inappropriate content.

7.4. When necessary, the Company may monitor your use of its systems on an individual basis but only where this is required because automated monitoring is not adequate or appropriate, for example where breach of this policy is suspected. This monitoring may include interception and/or recording of any email or Internet communications or telephone calls. The Company will give you written notification prior to carrying out such monitoring. In any event, any monitoring will be carried out in accordance with local laws.

7.5. The Company may in exceptional circumstances monitor your individual use of the IT Systems without notifying you. This will only be carried out where it is permitted by local law and only where it is necessary to withhold notification in order to make effective use of such monitoring or if it is required by law.

8. Training

8.1. The Company recognizes that an astute workforce is the best line of defense. We will provide security training opportunities and expert resources to help employees and contractors understand their obligations under this IS Policy and avoid creating undue risks. Employees must complete information security training within a reasonable time after initial hire. All workforce members must complete information security training on at least an annual basis. Managers must ensure that their employees complete all required training.

8.2. The Company may deem failure to participate in required training a violation of this IS Policy. The Company will retain attendance records and copies of security training materials delivered.

9. Client Policies

9.1. The Company may handle sensitive client information. In some cases, the Company may agree to comply with specific client information security policies or standards. To minimize special cases, the Company has developed this IS Policy to include the requirements common to most of our clients.

9.2. If the Company agrees to comply with additional client-specific information security policies or standards, we will notify affected workforce members. You must comply with any such policies or standards, including any related training or additional background screening requirements.

9.3. Legal and the Information Security Coordinator must review and approve any client agreements that require compliance with specific information security policies or standards.]

10. Data: Information Classification and Risk-Based Controls

The Company has established a three-tier classification scheme to protect information according to risk levels. The information classification scheme allows the Company to select appropriate security controls and balance protection needs with costs and business efficiencies.

All Company information may be classified as (from least to most sensitive): (1) Public Information, (2) Confidential Information, or (3) Highly Confidential Information.

Unless it is marked otherwise or clearly intended to be Public Information, treat all Company [and client] information as if it is at least Confidential Information, regardless of its source or form, including electronic, paper, verbal, or other information.

You must apply security controls appropriate for the assigned information classification level to all information you store, transmit, or otherwise handle. Use classification level markings, where feasible.

10.1. Public Information. Public Information is information that the Company has made available to the general public. Information received from another party (including a client) that is covered under a current, signed non-disclosure agreement must not be classified or treated as Public Information.

(a) Public Information Examples. Some Public Information examples include, but are not limited to:

(i) press releases;

(ii) Company marketing materials;

(iii) job announcements; and

(iv) any information that the Company makes available on its publicly-accessible website.

Do not assume that any information you obtain from the Company's internal network or systems is publicly available. For example, draft marketing materials are typically Confidential Information until their release. Consider all information to be at least Confidential Information, and not available for public disclosure without authorization, until you verify it is Public Information.

10.2. Confidential Information. Confidential Information is information that may cause harm to the Company, its clients, employees, or other entities or individuals if improperly disclosed, or that is not otherwise publicly available. Harms may relate to an individual's privacy, the Company's marketplace position or that of its clients, or legal or regulatory liabilities.

Mark Confidential Information to denote its status when technically feasible. Applications or databases that contain Confidential Information may be marked with an initial banner shown upon system access.

You must have authorization to disclose Confidential Information to an external party. Seek guidance from your manager or Legal prior to disclosing Confidential Information and verify that an appropriate non-disclosure or other agreement is in effect.

(a) Confidential Information Examples. Some Confidential Information examples include, but are not limited to:

(i) Company financial data, client lists, revenue forecasts, program or project plans, and intellectual property;

(ii) client-provided data, information, and intellectual property;

(iii) client contracts and contracts with other external parties, including vendors;

(iv) communications or records regarding internal Company matters and assets, including operational details and audits;

(v) Company policies, procedures, standards, and processes (for example, this IS Policy is Confidential Information and should not be shared without authorization from the Information Security Coordinator);

(vi) any information designated as "confidential" or some other protected information classification by an external party and subject to a current non-disclosure or other agreement;

(vii) information regarding employees (see also, Section 10.3, Highly Confidential Information, regarding personal information);

(viii) any summaries, reports, or other documents that contain Confidential Information; and

(ix) drafts, summaries, or other working versions of any of the above.

(b) Safeguards. You must protect Confidential Information with specific administrative, physical, and technical safeguards implemented according to risks, including (but not necessarily limited to):

(i) Authentication. Electronically stored Confidential Information must only be accessible to an individual after logging in to the Company's network.

(ii) Discussions. Only discuss Confidential Information in non-public places, or if a discussion in a public place is absolutely necessary, take reasonable steps to avoid being overheard.

(iii) Copying/Printing/Faxing/Scanning. Only scan, make copies, and distribute Confidential Information to the extent necessary or allowed under any applicable non-disclosure agreement or other applicable agreement. Take reasonable steps to ensure that others who do not have a business need to know do not view the information.

When faxing Confidential Information, use a cover sheet that informs the recipient that the information is the Company's Confidential Information. Set fax machines to print a confirmation page after sending a fax. Locate copiers, fax machines, scanners, and other office equipment in physically secured areas and configure them to avoid storing Confidential Information.

(iv) Encryption. You should encrypt Confidential Information when storing it on a laptop, smartphone, or other mobile device, including mobile storage devices. Consider encrypting Confidential Information when transmitting or transporting it externally, based on specific risks. Seek assistance from your manager if needed.

(v) Mailing. Use a service that requires a signature for receipt of the information when sending Confidential Information outside the Company]. When sending Confidential Information inside the Company, use a sealed security envelope marked "Confidential Information."

(vi) Meeting Rooms. You should only share Confidential Information in meeting rooms that are physically secured. Erase or remove any Confidential Information that you write on a whiteboard or other presentation tool upon the meeting's conclusion.

(vii) Need to know. Only access, share, or include Confidential Information in documents, presentations, or other resources when there is a business need to know.

(viii) Physical Security. Only house systems that contain Confidential Information, or store Confidential Information in paper or other forms, in physically secured areas.

10.3. Highly Confidential Information. Highly Confidential Information is information that may cause serious and potentially irreparable harm to the Company, its clients, employees, or other entities or individuals if disclosed or used in an unauthorized manner. Highly Confidential Information is a subset of Confidential Information that requires additional protection.

Mark Highly Confidential Information to denote its status when technically feasible. Applications or databases that contain Highly Confidential Information may be marked with an initial banner shown upon system access.

You may not remove Highly Confidential Information from the Company's environment without authorization.

You must have authorization to disclose Highly Confidential Information to an external party. Seek guidance from Legal and the Information Security Coordinator prior to disclosing Highly Confidential Information externally to ensure the Company meets its legal obligations.

(a) Highly Confidential Information Examples. Some Highly Confidential Information examples include, but are not limited to:

(i) personal information for employees, clients, business partners, or others; and

(ii) sensitive Company business information, such as budgets, financial results, or strategic plans.

(b) Safeguards. You must protect Highly Confidential Information with specific administrative, physical, and technical safeguards implemented according to risks and as prescribed by applicable laws, regulations, and standards, including (but not necessarily limited to):

(i) Authentication. Electronically stored Highly Confidential Information must only be accessible to an individual after logging in to the Company's network and with specific authorization.

(ii) Discussions. Only discuss Highly Confidential Information in non-public places.

(iii) Copying/ Printing/Faxing/Scanning. Do not scan, copy, or distribute Highly Confidential Information unless absolutely necessary. Take reasonable steps to ensure that others who do not have a specific business need to know do not view the information.

When faxing Highly Confidential Information, use a cover sheet that informs the recipient that the information is the Company's Highly Confidential Information. Set fax machines to print a confirmation page after sending a fax. Locate copiers, fax machines, scanners, and other office equipment in physically secured areas and configure them to avoid storing Highly Confidential Information.

(iv) Encryption. You must encrypt Highly Confidential Information when transmitting it, whether externally or internally, or when storing it on a laptop, smartphone, or other mobile device, including mobile storage devices such as USB drives. You should also encrypt Highly Confidential Information when storing it on a server, database, or other stationary device.

(v) Mailing. Do not mail Highly Confidential Information unless absolutely necessary. Use a service that requires a signature for receipt of the information when sending Highly Confidential Information outside the Company. When sending Highly Confidential Information inside the Company, use a sealed security envelope marked "Highly Confidential Information." If you use electronic media to mail Highly Confidential Information, you must encrypt and password protect it.

(vi) Meeting Rooms. You must only share Highly Confidential Information in meeting rooms that are physically secured. Erase any Highly Confidential Information that you write on a whiteboard or other presentation tool upon the meeting's conclusion.

(vii) Need to know. Only access, share, or include Highly Confidential Information in documents, presentations, or other resources when there is a specific business need to know.

(viii) Network Segmentation. You may only make Highly Confidential Information available to areas of the Company's network where there is a specific business need. Highly Confidential Information must be segmented from the rest of the Company's network through the use of controls such as firewalls, access control lists, or other security mechanisms.

(ix) Physical Security. Only house systems that contain Highly Confidential Information, or store Highly Confidential Information in paper or other forms, in physically secured areas, accessible only to those with a specific business need to know.

11. People: Roles, Access Control.

People are the best defense in information security. They are also the weakest link. The Company grants access to its systems and data based on business roles. The Company places limits on how you may use and interact with its information assets. These restrictions help lower risks and protect you and the Company.

11.1. Roles. Business roles and role-based access are based on the individual's relationship with the Company and assigned activities.

11.1.1. Employees. Human Resources provides employee screening and backgroundinvestigations. For more information, see HR PROCESSES. The Company may require employees who handle Highly Confidential Information to undergo additional background screening and testing where permitted by applicable laws.

Supervising managers may request access for their employees only to those Company IT systems and data required to meet business needs.

11.1.2. External Parties. The Company grants systems access to approved external parties, such as contractors, vendors, service providers, business partners, or others with a demonstrated business need that cannot be reasonably met through other means (see Section 14, Service Providers: Risks and Governance). The Company may support different access levels for different business situations.

[A sponsoring employee must be designated for any external party before the Company grants access to its systems or data. The sponsoring employee is responsible for supervising the external party, including compliance with this IS Policy.

The sponsoring employee may request access only to those Company resources necessary to meet business needs. The sponsoring employee must also request that any access granted be terminated when the business need ends.]

11.2. Identity and Access Management. The Company uses identity and access management controls to provide user accounts with appropriate privileges to employees and others. The Company will assign each individual a unique identifier using a standard algorithm (the individual's "primary ID"). You should only create device or application-specific identifiers if the primary ID cannot be used. Device or application-specific identifiers must be linked to an accountable individual.

11.2.1. Unique User Accounts. The Company assigns unique user accounts and passwords to individuals, using their primary ID. You must not share your account or password withothers. If system or other administrative accounts cannot be uniquely assigned to specific individuals, use mediated access, audit logs, or other technical controls to provide individual accountability.

11.2.2. Add, Change, Terminate Access. The Company restricts access to specific resources to those with a business need to know. Responsible managers [and sponsoring employees] should direct requests to add or change access levels to Group IT. System and application administrators must periodically review user accounts and access levels to confirm that a legitimate business need for the access still exists.

When an employee leaves the business, [Human Resources] must immediately notify Group IT. Group IT will timely deactivate the individual's account(s). [For external parties, the sponsoring employee must notify Group IT when there is no longer a business need for access to support timely account termination.] Managers should seek guidance from [Human Resources] and the Information Security Coordinator regarding access for employees on extended leaves.

11.2.3. Authorization Levels and Least Privilege. Proper authorization levels ensure that the Company only grants individuals the privileges they need to perform their assigned activities and no more. Known as least privilege access, this method minimizes risks. Least privilege applies to user and administrative access. You must not grant administrative privileges unless there is a specific business need and limit them to the extent feasible.

11.2.4. Role-Based Access Controls. Use role-based access control methods whenever feasible to assign authorization levels according to business functions, rather than uniquely for each individual. This method supports the least privilege approach by standardizing access. It also simplifies periodic access reviews.

12. Information Assets: Protecting and Managing the Company's Information Technology Environment. This section describes key safeguards that the Company uses to protect and manage its information technology (IT) environment. You must support their use to the extent that they apply to you.

12.1. Protecting Information Assets. Install and configure Company-owned computers according to current technical standards and procedures, including anti-virus software, other standard security controls, and approved operating system version and software patches. The Company supports preventive controls to avoid unauthorized activities or access to data, based on risk levels. The Company supports detective controls to timely discover unauthorized activities or access to data, including continuous system monitoring and event management.

12.1.1. End-User Computers and Access. Configure end-user computers to request authentication from the Company's domain at startup and user login. End-user computers may be denied network access if installed software versions do not match current standards. Users may not access the Company's network unless they have been properly authenticated.

Configure user accounts to require strong passwords. To protect against password guessing and other brute force attacks, the Company will deactivate user accounts after five failed login attempts. Reactivation may be based on a timeout or manual reset according to risk and technical feasibility.

Secure remote access points and require two-factor authentication. Encrypt authentication credentials during transmission across any network, either internal or external.

12.1.2. Passwords and User Credentials. Select strong passwords and protect all user credentials, including passwords, tokens, badges, smart cards, or other means of identification and authentication. Implement password rules so that users select and use strong passwords. Automate password rule enforcement to the extent technically feasible.

12.1.2.1. Minimum Password Rules. At minimum passwords must:

12.1.2.1.1. be at least 8 characters;

12.1.2.1.2. be comprised of a mix of letters (upper and lower case), numbers, and special characters (punctuation marks and symbols);

12.1.2.1.3. not be comprised of or use words that can be found in a dictionary;

12.1.2.1.4. not be comprised of an obvious keyboard sequence or common term (i.e., "qwerty," "12345678," or "password"); and

12.1.2.1.5. not include easily guessed data such as personal information about yourself, your spouse, your pet, your children, birthdays, addresses, phone numbers, locations, etc.

Several techniques can help you create a strong password. Substituting numbers for words is common. For example, you can use the numerals two or four with capitalization and symbols to create a memorable phrase. Another way to create an easy-to-remember strong password is to think of a sentence and use the first letter of each word as a password.

Treat passwords as Highly Confidential Information. You may be required to change your password periodically according to current Company standards. Change your password immediately and report the incident (see Section 13.1, Incident Reporting) if you have reason to believe that it has been compromised.

12.1.2.2. Password Protection. Protect your passwords at all times by:

12.1.2.2.1. Not disclosing your passwords to anyone, including anyone who claims to be from Group IT;

12.1.2.2.2. Not sharing your passwords with others (including co-workers, managers, clients, or family);

12.1.2.2.3. Not writing down your passwords or otherwise recording them in an unsecure manner;

12.1.2.2.4. Not using save password features for applications, unless provided or authorized by the Company;

12.1.2.2.5. Not using the same password for different systems or accounts, except where single sign on features are automated; and

12.1.2.2.6. Not reusing passwords.

Group IT procedures and technical standards define additional steps to protect passwords for administrative or device-specific accounts.

12.1.3. Perimeter Controls. Perimeter controls secure the Company's network against external attacks. Use firewalls, configured according to current technical standards and procedures, to separate the Company's trusted network from the internet or internet-facing environments.

The Company may implement additional perimeter controls including intrusion detection and prevention services, data loss prevention software, specific router or other network configurations, or various forms of network monitoring according to risks. Do not create internet connections outside perimeter controls.

12.1.4. Data and Network Segmentation. The Company may use technical controls, such as firewalls, access control lists, or other mechanisms, to segment some data or areas of its network according to risks. Segment Highly Confidential Information from the rest of the Company's network, to the extent technically feasible and reasonable. Do not alter network segmentation plans without approval from the Information Security Coordinator.

12.1.5. Encryption. The Company uses encryption to protect Confidential and Highly Confidential Information according to risks. Encryption may be applied to stored data (data-at-rest) and transmitted data (data-in-transit). Encrypting personal information may lower the Company's liability in the event of a data breach.

Only use generally accepted encryption algorithms and products approved by the Information Security Coordinator. Periodically review encryption products and algorithms for any known risks.

Laws may limit exporting some encryption technologies. Review the Company's Export Control Policy. Seek guidance from Legal prior to exporting or making any encryption technologies available to individuals outside the US.

12.1.5.1. Encryption Key Management. Encryption algorithms use keys to transform and secure data. Because they allow decryption of the protected data, proper key management is critical. Select encryption keys to maximize protection levels, to the extent feasible and reasonable. Treat them as Highly Confidential Information.

Ensure that keys are available when needed to support data decryption by using secure storage methods and creating and maintaining secure backups. Track access to keys. Keys should never be known or available to only a single individual. Change encryption keys on a periodic basis according to risks.

12.1.6. Data and Media Disposal. When the Company retires or otherwise removes computing, network, or office equipment (such as copiers or fax machines) or other information assets that may contain Confidential or Highly Confidential Information from the business, specific steps must be taken to scrub or otherwise render the media unreadable.

Simply deleting files or reformatting disks is not sufficient to prevent data recovery. Either physically destroy media, according to applicable waste disposal regulations, or scrub it using data wiping software that meets generally accepted data destruction standards. For example, see the National Institute of Standards and Technology's Special Publication 800-88, Guidelines for Media Destruction.

12.1.7. Log Management and Retention. The Company logs system and user activities onnetwork, computing, or other information assets according to risks. Security controls or other network elements may also produce logs.

Secure log data and files to prevent tampering and retain them according to the Company's Data Retention Schedule. Regularly review logs, using automated means where feasible, to identify any anomalous activities that may indicate a security incident.

12.1.8. Physical (Environmental) Security. The Company uses physical safeguards to avoid theft, intrusions, unauthorized use, or other abuses of its information assets. You must comply with the Company's current physical security policies and procedures (see Company Physical Security Policy) and:

12.1.8.1. position computer screens where information on the screens cannot be seenby unauthorized parties;

12.1.8.2. do not display Confidential and Highly Confidential Information on a computerscreen where unauthorized individuals can view it;

12.1.8.3. log off or shut down your workstation when leaving for an extended time period or at the end of your work day;

12.1.8.4. house servers or other computing or network elements (other than end-user equipment) in secure data centers or other areas approved by the Information SecurityCoordinator;

12.1.8.5. do not run network cabling through unsecured areas unless it is carrying only Public Information or otherwise protected data, such as encrypted data;

12.1.8.6. deactivate network ports that are not in use; and

12.1.8.7. store end-user devices that are not in use for an extended period of time in a secure area or securely dispose of them (see Section 12.1.6, Data and Media Disposal).

12.1.9. Disaster Preparedness (Business Continuity and Disaster Recovery). The Company develops, maintains, and periodically tests disaster preparedness plans. These plans support continuity of operations and systems availability if a disaster or other unplanned business impacting event occurs. The plans must be developed, reviewed, and tested according to the Company'sBusiness Continuity Planning Policy and Procedures/ Frontera Consulting Disaster Recovery and Business Continuity plan. Treat disaster preparedness plans as Confidential Information.

System administrators must perform regular data backups for the information assets they maintain according to the Company's Backup Policy and Procedures. When selecting a backup strategy, balance the business criticality of the data with the resources required and any impact to users and network resources. Protect backups according to the information classification level of the data stored. Document and periodically test restoration procedures.

12.2. Managing Information Assets. Group IT manages IT operations and related activities at the Company.

Only Company-supplied or approved software, hardware, and information systems, whether procured or developed, may be installed in the Company's IT environment or connected to the Company's network.

Group IT must approve and manage all changes to the Company's production IT environment to avoid unexpected business impacts. Direct questions regarding IT operations to John Lee. Development environments must comply with this IS Policy and current Group IT standards to minimize information security risks.

12.2.1. Procurement. Only Group IT, or those authorized by Group IT, may procure information assets for use in or connection to the Company's network. This IS Policy applies whether software or other assets are purchased, open source, or made available to the Company at no cost. Seek guidance from the Information Security Coordinator early in the software development process to identify and manage information security risks prior to implementation. Before using cloud computing services to access, store, or manage Confidential or Highly Confidential Information, you must obtain authorization from Legal and the Information Security Coordinator (see Section 3.7.3, Cloud Computing).

12.2.2. Asset Management. Track and document all information assets, including hardware, software, and other equipment, using the Company's asset management system(s). This inventory tracking should include operating system levels and all installed software and software versions to support vulnerability identification and mitigation (see Section 16.3, Vulnerability Management). Update the asset inventory as assets are removed from the business. Confidential or Highly Confidential Information must have an assigned data owner who is responsible for tracking its location, uses, and any disclosures. Properly dispose of all data and media to help avoid a breach of Confidential or Highly Confidential Information (see Section 12.1.6, Data and Media Disposal).

12.2.3. Authorized Environments and Authorities. Only authorized Group IT personnel, or other project personnel approved by Group IT, may install and connect hardware or software in the Company's IT environment. Do not convert end-user computers to servers or other shared resources without assistance from Group IT. Limit administrative, or privileged, systems access to those individuals with a business need to know. Group IT must distribute administrative access and information regarding administrative processes to more than one individual to minimize risks.

Internet connections and internet-facing environments present significant information security risks to the Company. The Information Security Coordinator must approve any new or changed internet connections or internet-facing environments.

12.2.4. Change Management. Group IT maintains a change management process to minimize business impact or disruptions when changes are made in the Company]'s production IT environment. Change requests must be accompanied by an action plan that includes assigned roles and responsibilities, implementation milestones, testing procedures, and a rollback plan, in the event the change fails.

Implement and maintain a change management process to track identified problems, fixes, and releases during software development. Design these processes to include code archiving (versioning) tools so that earlier versions can be recovered and rebuilt, if necessary.

12.2.5. [Application and Software Development. To avoid any undue or unexpected impact to the Company's production IT environment, application and software development activities, including system testing, must take place in reasonably segmented environments. Maintain segregation of duties between development and operations. Developers may be granted limited access to production environments where personnel and expertise availability is limited, but only for specific troubleshooting or support purposes. Software development must take place in authorized environments (see Section 12.2.3, Authorized Environments and Authorities).

Use security-by-design principles to identify potential information security risks and resolve them early in the development process. Seek guidance from the Information Security Coordinator, critical vendors, industry experts, and best practices to identify and avoid application-level security risks. Pay particular attention to protecting Highly Confidential Information through encryption or other appropriate means. Use defensive coding techniques and regular code review and application-level scanning to identify and remediate any information security issues before releasing software.]

13. Incident Reporting and Response. The Information Security Coordinator maintains a security incident reporting and response process that ensures management notifications are made based on the seriousness of the incident. The Information Security Coordinator investigates all reported or detected incidents and documents the outcome, including any mitigation activities or other remediation steps taken.

13.1. Incident Reporting. **Immediately notify Operations if you discover a security incident or suspect a breach in the Company's information security controls.** The Company maintains various forms of monitoring and surveillance to detect security incidents, but you may be the first to become aware of a problem. Early detection and response can mitigate damages and minimize further risk to the Company.

Treat any information regarding security incidents as Highly Confidential Information and do not share it, either internally or externally, without specific authorization.

13.1.1. Security Incident Examples. Security incidents vary widely and include physical and technical issues. Some examples of security incidents that you should report include, but are not limited to:

13.1.1.1. loss or suspected compromise of user credentials or physical access devices (including passwords, tokens, keys, badges, smart cards, or other means of identification and authentication);

13.1.1.2. suspected malware infections, including viruses, Trojans, spyware, worms, or any anomalous reports or messages from anti-virus software or personal firewalls;

13.1.1.3. loss or theft of any device that contains Company information (other than Public Information), including computers, laptops, tablet computers, smartphones, USB drives, disks, or other storage media;

13.1.1.4. suspected entry (hacking) into the Company's network or systems by unauthorized persons;

13.1.1.5. any breach or suspected breach of Confidential or Highly Confidential Information;

13.1.1.6. any attempt by any person to obtain passwords or other Confidential or Highly Confidential Information in person or by phone, email, or other means (sometimes called social engineering, or in the case of email, phishing); and

13.1.1.7. any other any situation that appears to violate this Policy or otherwise create undue risks to the Company's information assets.

13.1.2. Compromised Devices. If you become aware of a compromised computer or other device:

13.1.2.1. immediately deactivate (unplug) any network connections, but do not power down the equipment as valuable information regarding the incident may be lost if the device is turned off; and

13.1.2.2. immediately notify Operations.

13.2. Event Management. The Information Security Coordinator defines and maintains a security incident response plan to manage information security incidents. Report all suspected incidents, as described in this Policy, and then defer to the incident response process. Do not impede the incident response process or conduct your own investigation unless the Information Security Coordinator specifically requests or authorizes it.

13.3. Breach Notification. The law may require the Company to report security incidents that result in the exposure or loss of certain kinds of information to various authorities, affected individuals or organizations whose data was compromised, or both. Breaches of Highly Confidential Information (and especially personal information) are the most likely to carry these obligations (see Section 6, Data Protection). The Information Security Coordinator's incident response plan includes a step to review all incidents for any required breach notifications. Coordinate all external notifications with Legal and the Information Security Coordinator. Do not act on your own or make any external notifications without prior guidance and authorization.

14. Service Providers: Risks and Governance. The Information Security Coordinator maintains a service provider governance program to oversee service providers that interact with the Company's systems or Confidential or Highly Confidential Information. The service provider governance program includes processes to track service providers, evaluate service provider capabilities, and periodically assess service provider risks and compliance with this Policy.

14.1. Service Provider Approval Required. Obtain approval from Legal and the Information Security Coordinator before engaging a service provider to perform functions that involve access to the Company's systems or Confidential or Highly Confidential Information.

14.2. Contract Obligations. Service providers that access the Company's systems or Confidential or Highly Confidential Information must agree by contract to comply with applicable laws and this IS Policy or equivalent information security measures. The Company may require service providers to demonstrate their compliance with applicable laws and this Policy by submitting to independent audits or other forms of review or certification based on risks.

15. [Client Information: Managing Intake, Maintenance, and Client Requests. The Company frequently creates, receives, and manages data on behalf of our clients. With guidance from the Information Security Coordinator, each business unit develops, implements, and maintains an appropriate process and procedures to manage client data intake and protection.

Business unit-specific client data intake and protection processes may vary but must include, at minimum, means for (1) identifying client data and any pertinent requirements prior to data intake or creation; (2) maintaining an inventory of client data created or received; and (3) ensuring the Company implements and maintains appropriate information security measures, including proper data and media disposal when the Company no longer has a business need to retain the client data (or is no longer permitted to do so by client agreement).

15.1. Requirements Identification. Identify any pertinent client data requirements prior to data intake or creation according to your business unit's client data intake and protection process. Requirements may be contractual, the result of applicable law or regulations, or both (see Section 6, Data Protection).

15.2. IntakeManagement. Business unit-specific client data intake processes and procedures must provide for secure data transfer. Maintain an inventory of client data that includes, at a minimum:

15.2.1. a description of the client data;

15.2.2. the location(s) where the data is stored;

15.2.3. who is authorized to access the data (by category or role, if appropriate);

15.2.4. whether the data is Confidential or Highly Confidential Information;

15.2.5. how long the data is to be retained (using criteria, if appropriate); and

15.2.6. any specific contractual or regulatory obligations or other identified data protection or management requirements.

Treat any client-provided personal information as Highly Confidential Information (see Section 10.3, Highly Confidential Information). To minimize risks for clients and the Company, engage clients in an ongoing dialogue to determine whether business objectives can be met without transferring personal information to the Company.

15.3. Client Data Protection. Protect all client data the Company creates or receives in accordance with this IS Policy and the data's information classification level, whether Confidential or Highly Confidential Information, in addition to any specific client-identified requirements.

15.4. Client Data and Media Disposal. Ensure that any client data, or media containing client data, is securely disposed of when it is no longer required for Company business purposes, or as required client agreement (see Section 12.1.6, Data and Media Disposal). Update the applicable business unit client data inventory accordingly.]

16. Risk and Compliance Management. The Company supports an ongoing risk management action cycle to (1) enforce this IS Policy; (2) identify information security risks; (3) develop procedures, safeguards, and controls; and (4) verify that safeguards and controls are in place and working properly.

16.1. Risk Assessment and Analysis. The Company maintains a risk assessment program to identify information security risks across its IT environment, including application software, databases, operating systems, servers, and other equipment, such as network components. The Information Security Coordinator coordinates risk assessment activities that may take several forms, including analyses, audits, reviews, scans, and penetration testing. **Do not take any actions to avoid, impact, or otherwise impede risk assessments.**

Only the Information Security Coordinator is authorized to coordinate risk assessments. Seek approval from Legal and the Information Security Coordinator prior to engaging in any risk assessment activities or disclosing any assessment reports outside the Company.

16.2. Remediation and Mitigation Plans. The Information Security Coordinator maintains and oversees remediation and mitigation plans to address risk assessment findings according to risk levels.

16.3. Vulnerability Management. Manufacturers, security researchers, and others regularly identify security vulnerabilities in hardware, software, and other equipment. In most cases, the manufacturer or developer provides a patch or other fix to remediate the vulnerability. In some situations, the vulnerability cannot be fully remediated, but configurations can be changed or other steps taken to mitigate the risk created.

The Information Security Coordinator maintains a process to identify and track applicable vulnerabilities, scan devices for current patch status, and advise system administrators. Schedule any necessary updates using standard change management processes (see Section 12.2.4, Change Management) and according to risk level. Make all Company-owned devices available to Group IT for timely patching and related activities.

16.4. Compliance Management. The Company maintains compliance management processes to enforce this IS Policy. The Company may automate some monitoring and enforcement processes.] If compliance management processes indicate that you may have acted contrary to this IS Policy, you may [receive an automated notification or] be contacted by the Information Security Coordinator to explain. In some cases, the Information Security Coordinator may contact your supervising manager or Human Resources to resolve the issue.

17. Effective Date. This Information Security Policy is effective as o

17.1. Revision History. Original Publication.

18. Consequences of Breach

18.1. Compliance with this policy is a requirement of your employment and any breach of it will be treated as a serious disciplinary issue and will be dealt with in accordance with the Company’s disciplinary procedure. Serious breaches of this policy may be considered gross misconduct resulting in immediate termination of your employment. If the Company suspects illegal activities, it may report them to the applicable authorities and aid in any investigation or prosecution of the individuals involved.

ACKNOWLEDGEMENT

Acknowledgement of Receipt and Review

I,________________________(employee name), acknowledge that on____________(date), I received and read a copy of the Company's Information Security Policy, dated [VERSION DATE] and understand that it is my responsibility to be familiar with and abide by its terms. This IS Policy is not promissory and does not set terms or conditions of employment or create an employment contract

Signed________________________________ Dated ___________________

Name ________________________________