DRAFT WISP

Document Information

Document Version	1.0
Document Status	
Document Owner	TECOBI LLC
Changes Compared to Previous Version	None
Related Documents	Written Information Security Plan
Distribution	
Effective Date	
Last Updated	

TECOBI, LLC

INFORMATION SECURITY POLICY

Effective Date: March 23, 2023

Last Revised: ___N/A_____

1. Introduction: ISP Foundation and Regulatory Compliance. This Information Security Policy ("ISP") promotes a balance between information security practices and business needs. The ISP helps TECOBI, LLC ("TECOBI") meet our legal obligations. From time to time, TECOBI may implement different levels of security controls for different information assets (including computer systems and data), based on risk and other considerations. This ISP sets forth the security protocols put in place by TECOBI and is intended for use by TECOBI 's Information Technology and Security Team (IT) members. No single ISP can cover all the possible information security issues TECOBI may face.

This ISP is Confidential Information.

Our customers, 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 TECOBI. Strong information security requires diligence by everyone, and it is part of everyone's job.

1.1 Guiding Principles. TECOBI follows these guiding principles when developing and implementing information security controls:

(a) TECOBI strives to protect the confidentiality, integrity and availability of its information assets and those of its employees and clients.

(b) We will comply with applicable privacy and data protection laws.

(c) We will balance the need for business efficiency with the need to protect sensitive, proprietary or other confidential information from undue risk.

(d) We will grant access to sensitive information only after training employees on how to properly protect such information from unauthorized disclosure.

(e) 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.

Scope. This ISP applies to all of TECOBI. This ISP provides detailed information security guidance that you must follow in addition to any obligations listed in our ALG DIRECT DBA TECOBI

1.1 Employee Handbook.

From time to time, TECOBI may approve and make available more detailed policies, procedures, standards and processes to address specific information security issues. Those additional policies, procedures, standards and processes are extensions to this ISP.

1.2 Resources. TECOBI's goal is to balance information security with accomplishing business goals. Many effective administrative, physical, and technical safeguards are available. Employees are required to seek guidance before taking any action(s) that may create information security risks

1.3 Regulatory Compliance. Various information security laws, regulations and industry standards apply to TECOBI and the data we handle. TECOBI is committed to complying with all applicable laws, regulations, and standards. For example, certain laws protect individuals' personal

data. Many jurisdictions have enacted breach notification laws that require organizations to notify affected individuals if personal data is lost or accessed by unauthorized parties. Some jurisdictions have enacted data protection laws that require organizations to protect personal data using reasonable data security measures or more specific means. These laws may apply to personal data for TECOBI employees, customers, investors, business partners and others.

2. Responsibilities: Security Organization, Authority and Obligations. TECOBI recognizes the need for a strong information security program.

2.1 Information Security Coordinator(s). The Information Security Coordinator(s) will enforce TECOBI information security program.

2.2 ISP Authority and Maintenance. TECOBI has granted the Information Security Coordinator(s) the authority to develop, maintain and enforce this ISP and any additional policies, procedures, standards and processes, as deemed necessary and appropriate.

2.3 ISP Review. On at least an annual basis, the Information Security Coordinator will initiate a review of this ISP, with Outside General Counsel and other TECOBI stakeholders, as appropriate.

2.4 Training. TECOBI recognizes that an astute workforce is the best line of defense. We will provide security training opportunities and the Information Security Coordinator will be available to help employees, and service providers understand their obligations under this ISP and avoid creating undue risks. Employees must complete information security training within a reasonable time after initial hire. All workforce members must complete regular information security training annually and ad hoc training as required.

All employees must complete operation and technical onboarding and offboarding when hired or terminated from TECOBI.

3. Data: Information Classification and Risk-Based Controls. TECOBI has established a three-tier classification scheme to protect information according to risk levels. The information classification scheme allows TECOBI to select appropriate security controls and balance protection needs with costs and business efficiencies.

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

3.1 Public Information. Public Information is information that TECOBI has made available to the general public, and/or information made available from federal, state, or local government records.

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

(i) press releases;

(ii) TECOBI marketing materials;

(iii) job announcements; and

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

Do not assume that any information you obtain from TECOBI internal network or systems is publicly available. Consider all information to be at least Confidential Information and not available for public disclosure without authorization, until you verify it is Public Information.

3.2 Confidential Information. Confidential Information is information that may cause harm to TECOBI, 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, TECOBI reputation or that of its clients or legal or regulatory liabilities.

Mark Confidential Information to denote its status when technically feasible.

You must have authorization to disclose Confidential Information to an external party. Seek guidance from the Information Security Coordinator or Outside General Counsel prior to disclosing Confidential Information and verify that an appropriate non-disclosure or other agreement is in effect.

(a) Confidential Information Examples. Confidential Information examples includes:

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

(ii) employee data, information and intellectual property;

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

(iv) any information directly related to past, current, or contemplated litigation;

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

(vi) TECOBI policies, procedures, standards and processes (for example, this ISP is Confidential Information and should not be shared without authorization from the Information Security Coordinator);

(vii) 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;

(viii) information regarding employees (see also, Section 3.3, Highly Confidential Information, regarding personal data);

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

(x) 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 TECOBI 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) Mailing. Use a service that requires a signature for receipt of the information when sending Confidential Information outside TECOBI.

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

(v) Copying/Printing/Scanning. Copiers, scanners, and other office equipment are in physically secured areas and configured to avoid storing Highly Confidential Information.

3.3 Highly Confidential Information. Highly Confidential Information is information that may cause serious and potentially irreparable harm to TECOBI and its 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.

You may not remove Highly Confidential Information from TECOBI 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 TECOBI meets its legal obligations.

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

(i) personal data for employees (e.g., HR data), business partners or others; and

(ii) sensitive TECOBI business information, such as budgets, legal, 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 TECOBI 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 TECOBI 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) 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 TECOBI. If you use electronic media to email Highly Confidential Information, you must encrypt and password protect it.

(v) 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 and depending on the business function of the data and individual.

4. People: Roles, Access Control and Acceptable Use. People are the best defense in information security. They are also the weakest link. TECOBI grants access to its systems and data based on business roles. TECOBI places limits on how you may use and interact with its information assets. These restrictions help lower risks and protect you and TECOBI.

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

(a) Employees. Access for employees is granted only to those TECOBI systems and data required to meet business needs.

(b) External Parties. TECOBI grants systems access to approved external parties, such as service providers, with a demonstrated business need that cannot be reasonably met through other means (see Section 7, Service Providers: Risks and Governance). TECOBI may support different access levels for different business situations.

4.2 Identity and Access Management. TECOBI uses identity and access management controls to provide user accounts with appropriate privileges to employees, consultants, and others. TECOBI 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.

(a) Unique User Accounts. TECOBI assigns unique user accounts and passwords to individuals, using their primary ID. You must not share your account or password with others. 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.

(b) Add, Change, Terminate Access. TECOBI restricts access to specific resources to those with a business need to know. User accounts and access levels must be periodically reviewed to confirm that a legitimate business need for the access still exists.

When an employee or consultant leaves TECOBI, the employee’s Manager/Supervisor must notify Human Resources (HR). HR must notify IT to deactivate the individual's account(s). Access should be terminated as closely as possible to the termination date/time, but in no case greater than one calendar date from the termination date/time. Managers should seek guidance from HR and IT regarding access for employees on extended leaves.

(c) Authorization Levels and Least Privilege. Proper authorization levels ensure that TECOBI 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.

(d) 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.

4.3 Acceptable Use ISP. TECOBI provides employees and others with network resources and systems to support its business requirements and functions. This section limits how you may use TECOBI information assets and explains the steps you must take to protect them.

If you have any questions regarding acceptable use of TECOBI resources, please discuss them with your manager or contact the Information Security Coordinator for additional guidance.

(a) Desktop, Laptop and End-User Controls. You may only access TECOBI network using approved end-user devices that support our current minimum information security standards. Standards for end-user devices may include protective controls and specific configurations, such as anti-virus software, patching levels and required operating system or other software versions. TECOBI owned machines may be configured to automatically receive upgrades. You may be denied remote access using non TECOBI owned devices that do not meet current standards.

Use your own TECOBI provided account(s) to access TECOBI network and systems, unless you have been specifically authorized to use a device-specific, administrative, or other account (see Section 4.2, Identity and Access Management).

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.

(b) Information Handling and Storage. You must properly handle, store and securely dispose of TECOBI information. 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 TECOBI 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 TECOBI information, including hard drives, 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 to IT for secure disposal when it is no longer required to meet business needs.

(c) Internet Use: Email, Messaging, Social Media and Cloud Computing. The internet offers a variety of services that TECOBI employees, consultants, and service providers depend on to work effectively. However, some technologies create undue risks to TECOBI assets. Some uses are not appropriate in the workplace.

TECOBI 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 TECOBI resources.

(i) 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 ISP. Internet use must comply with this ISP.

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

Do not use internet-based remote access services to access TECOBI network or systems, including desktop computers. If you need remote access, use TECOBI provided or authorized software (see Section 4.3(f), Remote Access).

(ii) 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 3, Data: Information Classification and Risk-Based Controls). Do not make postings or send messages that speak for TECOBI or imply that you speak for TECOBI 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.

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. TECOBI 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 3, 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 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.

(iii) Cloud Computing. TECOBI 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 TECOBI ability to comply with some laws. Before using any cloud computing services to collect, create, store, or otherwise manage TECOBI Confidential or Highly Confidential Information, you must obtain approval from the Information Security Coordinator (see Section 7, Service Providers: Risk and Governance).

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

(d) 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 TECOBI information assets, so you must take appropriate steps to protect them.

TECOBI 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 ISP and any additional policies, procedures, standards and processes TECOBI 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).

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 TECOBI email, must be protected using a password or other approved authentication method.

(e) Remote Access. If you have a business need to access TECOBI network and systems from home, while traveling, or at another location, TECOBI may grant you remote access.

(f) External Network Connections. Some business situations may require creating a secure connection from TECOBI network to an external party's network (extranet). Examples include working with systems, outsourcing, or partnering with another organization for an extended period of time (for example NTT Corporation for ERP Hosting). 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 to TECOBI network before implementation. A signed business agreement between the two organizations must accompany any extranet connection.

(g) Wireless Network Connections. Do not connect any wireless access points, routers or other similar devices to TECOBI network unless IT has reviewed and approved them.

Secure and maintain approved wireless network (WiFi) connections according to current TECOBI technical and physical security standards. Do not connect wireless access points (WAPs) directly to TECOBI 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.

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

5.1 Protecting Information Assets. TECOBI supports preventive controls to avoid unauthorized activities or access to data, based on risk levels. TECOBI supports detective controls

to timely discover unauthorized activities or access to data, including continuous system monitoring and event management.

(a) End-User Computers and Access.

Configure user accounts to require strong passwords. To protect against password guessing and other brute force attacks, TECOBI 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. Encrypt authentication credentials during transmission across any network, either internal or external.

(b) 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.

(i) Password Rules. Microsoft complexity standards are used. At minimum passwords must:

(A) be at least 7 characters;

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

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 TECOBI standards. Change your password immediately and report the incident (see Section 6.1, Incident Reporting) if you have reason to believe that it has been compromised.

(ii) Password Protection. Protect your passwords at all times by:

(A) Not disclosing your passwords to anyone, including anyone who claims to be from IT;

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

(C) Not writing down your passwords or otherwise recording them in an unsecure manner;

(D) Not using save password features for applications, unless provided or authorized by TECOBI;

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

(F) Not reusing passwords.

(c) Perimeter Controls. Perimeter controls secure TECOBI network against external attacks. Use firewalls, configured according to current technical standards and procedures, to separate TECOBI trusted network from the internet or internet-facing environments.

(d) Physical (Environmental) Security. TECOBI uses physical safeguards to avoid theft, intrusions, unauthorized use, or other abuses of its information assets. You must:

(i) position computer screens where information on the screens cannot be seen by unauthorized parties;

(ii) not display Confidential and Highly Confidential Information on a computer screen where unauthorized individuals can view it;

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

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

(v) not run network cabling through unsecured areas unless it is carrying only Public Information or otherwise protected data, such as encrypted data; and

(vi) 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 5.1(e), Data and Media Disposal).

IT must perform regular data backups for the information assets they maintain.

5.2 Managing Information Assets. IT manages IT operations and related activities at TECOBI.

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

IT must approve and manage all changes to TECOBI production IT environment to avoid unexpected business impacts. Direct questions regarding IT operations to TECOBI IS Global Applications Management Development environments must comply with this ISP and the Information Systems Control ISP standards to minimize information security risks.

(a) Procurement. Only IT, or those authorized by IT, may procure information assets for use in or connection to TECOBI network. This ISP applies whether software or other assets are purchased, open source, or made available to TECOBI at no cost.

(b) Asset Management. Track and document all information assets, including hardware, software and other equipment. This inventory tracking should include operating system levels and all installed software and software versions to support vulnerability identification and mitigation (see Section 9.2, 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 5.1(e), Data and Media Disposal).

(c) Authorized Environments and Authorities. Only authorized IT personnel, or other project personnel approved by IT, may install and connect hardware or software in TECOBI IT environment. Do not convert end-user computers to servers or other shared resources without assistance from IT. Limit administrative, or privileged, systems access to those individuals with a business need to know. 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 TECOBI. IT must approve any new or changed internet connections or internet-facing environments.

(d) Change Management. Any change to an existing infrastructure, network, or computerized system managed or supported by TECOBI must approved by the Information Security Coordinator.

6. Incident Reporting and Response. IT investigate all reported or detected incidents and document the outcome, including any mitigation activities or other remediation steps taken.

6.1 Incident Reporting. **Immediately notify the Information Security Coordinator at** privacy@tecobi.com **if you discover a security incident or suspect a breach in TECOBI information security controls.** TECOBI 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 TECOBI.

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

(a) 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:

(i) 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);

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

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

(iv) suspected entry (hacking) into TECOBI network or systems by unauthorized persons;

(v) any breach or suspected breach of Confidential or Highly Confidential Information;

(vi) 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

(vii) any other any situation that appears to violate this ISP or otherwise create undue risks to TECOBI information assets.

(b) Compromised Devices. If you become aware of a compromised computer or other device:

(i) 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

(ii) immediately notify IT.

6.2 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 ISP 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 or General Counsel specifically requests or authorizes it.

6.3 Breach Notification. The law may require TECOBI to report security incidents that result in the exposure or loss of certain kinds of information or that affect certain services or infrastructure to various authorities, affected individuals or organizations whose data was compromised, or both. Breaches of Highly Confidential Information (and especially personal data) are the most likely to carry these obligations (see Section 1.5, Regulatory Compliance). Coordinate all external notifications with IT and the Information Security Coordinator. Do not act on your own or make any external notifications without prior guidance and authorization.

7. Service Providers: Risks and Governance. TECOBI has processes to evaluate service provider capabilities and periodically assess service provider risks and compliance with this ISP.

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

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

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

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

8.1 Requirements Identification. Identify any pertinent employee and client data requirements prior to data intake or creation according to your business unit's employee and client data intake and protection process. Requirements may be contractual, the result of applicable law or regulations, or both (see Section 1.5, Regulatory Compliance).

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

(a) a description of the employee and client data;

(b) the location(s) where the data is stored;

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

(d) whether the data is Confidential or Highly Confidential Information;

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

(f) any specific contractual or regulatory obligations or other identified data protection or management requirements.

Treat any employee and client-provided personal data as Highly Confidential Information (see Section 3.3, Highly Confidential Information). To minimize risks for employees, clients and TECOBI, engage clients in an ongoing dialogue to determine whether business objectives can be met without transferring personal data to TECOBI.

8.3 Data Protection. Protect all employee and client data TECOBI creates or receives in accordance with this ISP and the data's information classification level, whether Confidential or Highly Confidential Information, in addition to any specific client-identified requirements.

8.4 Data and Media Disposal. Ensure that any employee and client data, or media containing employee and client data, is securely disposed of when it is no longer required for TECOBI business purposes, or as required by the employee or client agreement (see Section 5.1(e), Data and Media Disposal). Update the applicable business unit employee and client record of processing accordingly.

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

9.1 Risk Assessment and Analysis. TECOBI 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. **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 the Information Security Coordinator prior to engaging in any risk assessment activities or disclosing any assessment reports outside TECOBI.

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

9.3 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.

IT 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 5.2(d), Change Management) and according to risk level. Make all TECOBI owned devices available to IT for timely patching and related activities.

9.4 Compliance Management. TECOBI maintains compliance management processes to enforce this ISP. If compliance management processes indicate that you may have acted contrary to this ISP, you may be contacted by the Information Security Coordinator to explain.

10. Effective Date. This Information Security ISP is effective as of the Effective Date set forth on the first page.

Data Processing Addendum

This Data Processing Addendum ("**Addendum**") is entered into by and between {**NAME of Customer}**("**Company**") and TECOBI ("**Service Provider**") and is effective as of the date of the last signature below ("**Effective Date**").

This Addendum forms a part of the Master Services agreement between Company and Service Provider, dated xx/xx/xxxx (the "**Agreement**") related to Service Provider's provision of certain services (the "**Services**"). Except as modified herein, the terms of the Agreement shall remain in full force and effect.

The parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Agreement.

1. Definitions. For purposes of this Addendum, the following terms will have the meanings set forth below. Capitalized terms used but not otherwise defined in this Addendum will have the meaning given to them in the Agreement.

1.1. "Affiliate" means an entity that owns or controls, is owned or controlled by, or is under common control or ownership with, either Company or Service Provider respectively. "Control," for purposes of this definition, means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

1.2. "Company Personal Data" means any Personal Data Processed by Service Provider or a Subprocessor on behalf of Company.

1.3. "Data Protection Laws" means any and all laws, rules and regulations related to privacy, security, data protection, and/or the Processing of Personal Data, in any relevant jurisdiction, each as amended, replaced or superseded from time to time.

1.4. "Data Subject" means the identified or identifiable person to whom Personal Data relates.

1.5. "Personal Data" means (a) information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular person or household; and (b) any information defined as "personal data", "personal information," or other similar terms under applicable Data Protection Laws.

1.6. "Personal Data Breach" means the accidental, unauthorized, or unlawful destruction, loss, alteration, disclosure of, or access to, Company Personal Data transmitted, stored or otherwise Processed by Service Provider or any Subprocessor.

1.7. "Processing" means any operation or set of operations that is performed upon Personal Data, whether or not by automatic means, such as access, collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, return or destruction. The terms "Process," "Processes" and "Processed" will be construed accordingly.

1.8. "Processor" means any person or entity which Processes Company Personal Data, including as applicable any "service provider" or "contractor" as those terms are defined by applicable Data Protection Laws.

1.9. "Regulator" means any independent public authority, government agency, and any similar regulatory authority responsible for the enforcement of Data Protection Laws.

1.10. "Subprocessor" means any Processor (including any third party and any Service Provider Affiliate) appointed by or on behalf of Service Provider who may Process Company Personal Data.

2. Processing of Personal Data

2.1. The parties acknowledge and agree that Company at all times retains control of Company Personal Data. As between the parties, all Company Personal Data is and shall remain the property of Company and all rights, title and interest in and to the Company Personal Data shall remain with Company.

2.2. Subject to Service Provider's compliance with this Addendum, Company agrees to make Company Personal Data available to Service Provider for the limited and specified purpose of providing the Services as contemplated by the Agreement. Company reserves the right to take reasonable and appropriate steps to help ensure that Service Provider Processes Company Personal Data in a manner consistent with Company's obligations under Data Protection Laws, including without limitation, the right upon notice to stop and remediate any unauthorized Processing of Company Personal Data.

2.3. Service Provider acknowledges and agrees that, with regard to the Processing of Company Personal Data, Service Provider is acting as a Processor. Service Provider further certifies that Service Provider (a) understands the obligations and restrictions imposed on it by applicable Data Protection Laws in its role as a Processor; (b) will comply with all such obligations, including providing the same level of privacy protection as required by applicable Data Protection Laws; and (c) will notify Company if Service Provider determines it can no longer meet its obligations under applicable Data Protection Laws or this Addendum.

2.4. Service Provider will only Process Company Personal Data on behalf of Company (a) to the extent, and in such a manner, as is necessary for the purposes of fulfilling its obligations under the Agreement; and (b) in accordance with the terms of the Agreement and this Addendum, which together constitute Company's instructions. The restrictions set forth in this section shall not restrict Service Provider's ability to Process Company Personal Data where required to do so by applicable laws to which Service Provider is subject; provided, however, Service Provider shall promptly notify Company of such legal requirement before Processing, unless such law prohibits such notification.

2.5. Without limiting Service Provider's obligations under Section 2.3, Service Provider will not:

2.5.1. retain, use, or disclose Company Personal Data for any purpose other than to perform its obligations under the Agreement, which for the avoidance of doubt prohibits Service Provider from retaining, using, or disclosing Company Personal Data outside of the direct business relationship with Company or for any other purpose;

2.5.2. "sell" or "share" (as those terms are defined by applicable Data Protection Laws) Company Personal Data; or

2.5.3. combine Company Personal Data with Personal Data Service Provider receives from or on behalf of another person or entity or collects from its own interactions with a Data Subject except to perform a business purpose as defined in regulations adopted pursuant to Cal. Civ. Code 1798.185(a)(10).

2.6. The subject-matter of Processing of Company Personal Data by Service Provider is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, and the types of Personal Data Processed under this Addendum are further specified in **Exhibit 1** to this Addendum.

3. **Service Provider Personnel**. Service Provider will take reasonable steps to ensure that access to Company Personal Data is limited to those of its Affiliates, employees, agents, and subcontractors who (a) have a need to know or otherwise access Company Personal Data to enable Service Provider to perform its obligations under the Agreement and this Addendum, and (b) who are bound in writing by confidentiality obligations sufficient to protect the confidentiality of Company Personal Data in accordance with the terms of this Addendum.

4. **Security**. Service Provider shall implement and maintain appropriate technical and organizational safeguards to protect Company Personal Data and will ensure that all such safeguards comply with applicable Data Protection Laws. In assessing the appropriate level of security, Service Provider will take into account the risks that are presented by Processing, in particular from accidental, unauthorized, or unlawful destruction, loss, alteration, damage, disclosure of, or access to Company Personal Data transmitted, stored, or otherwise Processed. Upon Company's request, Service Provider will provide its Written Information Security Plan to demonstrate its security practices.

5. Personal Data Breach

5.1. In the event of a Personal Data Breach impacting Company Personal, Service Provider will (a) notify Company within forty-eight (48) hours after Service Provider or any Subprocessor becomes aware of such Personal Data Breach; (b) provide Company with sufficient details of the Personal Data Breach to allow Company to meet any obligations under Data Protection Laws to report or inform Data Subjects or relevant Regulators of the Personal Data Breach; and (c) cooperate, and require any Subprocessor to cooperate, with Company in the investigation, mitigation, and remediation of any such Personal Data Breach.

6. Subprocessors

6.1. Service Provider will not engage any Subprocessor without notifying Company and obtaining Company's prior written authorization. Notwithstanding the foregoing, Company hereby authorizes those Subprocessors listed in **Exhibit 1** to this Addendum, provided that any subsequent changes to the list of pre-approved Subprocessors must be authorized by Company.

6.2. With respect to any authorized Subprocessor, Service Provider will:

6.2.1. enter into a written agreement with each Subprocessor containing the same obligations imposed on Service Provider under this Addendum and applicable Data Protection Laws with respect to Company Personal Data; and

6.2.2. remain fully liable to Company for the acts or omissions of its Subprocessors.

7. Data Subject Rights

7.1. Service Provider will notify Company if it receives a request from a Data Subject regarding Company Personal Data, including a request by a Data Subject to exercise a right under Data Protection Laws.

7.2. Service Provider will assist Company in fulfilling Company's obligations to respond to such requests, including at minimum, maintaining the ability to access, modify, remove from Processing, or irrevocably delete or destroy the Personal Data of an individual Data Subject when requested by Company.

7.3. Should the Service Provider or any Subprocessor directly perform any data collection from Data Subjects in connection with the Company's instructions, the Service Provider will ensure that Data Subjects receive the Company's Privacy Policy at or before the point at which any information is collected about the Data Subject.

8. Deletion or Return of Company Personal Data

8.1. At any time during the term of the Agreement at Company's request, or upon the termination or expiration of the Agreement for any reason, Service Provider will, and will instruct all Subprocessors to, (a) return to Company all copies of Company Personal Data in its possession, or the possession of such Subprocessor, or (b) delete and procure the deletion of all other copies of Company Personal Data Processed by Service Provider or any Subprocessor within one hundred and eighty one (181) days. Company agrees that it is necessary for Service Provider to retain Company Personal Data for this time period for reasons set forth in the Agreement. Service Provider will comply with all reasonable directions provided by Company with respect to the return or deletion of Company Personal Data.

8.2. Notwithstanding Section 8.1 above, Service Provider may retain Company Personal Data if required by applicable Data Protection Laws, but only to the extent and for such period as required by such legal requirement. Service Provider will notify Company in writing if it believes that such a legal requirement exists. If required by law to retain Company Personal Data, Service Provider will continue to ensure the security and confidentiality of such Company Personal Data and only Process such Company Personal Data as necessary for the purpose specified in the applicable Data Protection Laws requiring such storage.

9. Compliance and Audits

9.1. Upon Company's request, Service Provider will provide such assistance as Company reasonably requires in ensuring compliance with Company's obligations under applicable Data Protection laws, including but not limited to any data protection impact assessments and any prior consultations with any Regulator where required.

9.2. In addition to any audit rights Company may have under the Agreement, Service Provider will make available to Company all information necessary to demonstrate Service Provider's compliance with this Addendum, as well as any applicable Data Protection Laws, and will allow for and contribute to audits, including inspections, by Company, or a third-party auditor mandated by Company, in order to assess Service Provider's compliance. Service Provider will fully cooperate with such audits or assessments by providing reasonable access to knowledgeable personnel; physical premises; and any relevant records, documentation, processes, and systems in order that Company may satisfy itself of Service Provider's compliance with this Addendum.

10. **Changes in Data Protection Laws**. If any variation is required to this Addendum as a result of a change in or subsequently applicable Data Protection Laws, the parties agree to discuss and negotiate in good faith any variations to this Addendum necessary to address such changes, with a view to agreeing and implementing those or alternative variations as soon as practicable.

11. **General Terms**. Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum will remain valid and in force. The invalid or unenforceable provision will be either: (a) amended as necessary to ensure its validity and enforceability, while preserving the intent of the provision as closely as possible or, if this is not possible, (b) construed in a manner as if the invalid or unenforceable part had never been contained therein. This Addendum and the other portions of the Agreement will be read together and construed, to the extent possible, to be in concert with each other. In the event of any conflict between the Agreement and this Addendum, this Addendum will govern with respect to the subject matter of this Addendum.

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Agreement as of the Effective Date.

COMPANY:	**SERVICE PROVIDER**:
{company name}	**TECOBI, LLC**
Signature: _____	Signature: _____
Name: _____	Name: Alana Foley-Greenwood
Title: _____	Title: Controller

List of Exhibits:

Exhibit 1: Details of Processing

Exhibit 1

Details of Processing

1. Subject Matter of Processing

The subject-matter of Processing of Company Personal Data by Service Provider is the performance of the Services pursuant to the Agreement.

2. Nature and Purpose of Processing

Company Personal Data will be Processed as necessary to perform the Services pursuant to the Agreement and will be subject to the processing activities described in any Statement of Work or Order Form that makes reference to, is incorporated under, or is subject to the Agreement.

3. Duration of Processing

Subject to section 8 of the Addendum, Service Provider will Process Company Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

4. Types of Personal Data

The types of Company Personal Data shall be as is contemplated or related to the Processing described in any Statement of Work or Order Form that makes reference to, is incorporated under, or is subject to the Agreement.

5. List of Subprocessors

The following table sets out the list of Subprocessors that Company has specifically authorized as of the Effective Date.

Entity Name	Entity Country	Description of Service/Processing Activity
Google	USA	Server Hosting
Twilio	USA	Telephony Provider
Bandwidth	USA	Telephone Provider