

iTech Solutions, Inc. Policy Handbook

[Table of Contents](#)

Policy Name:	Employee Confidentiality Policy		
Policy Number:		Applies to:	
Date Adopted:		Date Modified:	

Policy brief & purpose

iTech's confidentiality policy refers to the disclosure of important information. During the course of everyday business, employees will unavoidably receive and handle personal and private information about clients, partners and iTech. This policy is designed to set the rules that will protect this information from exposure.

Scope

This policy affects all employees and others that may have access to confidential information, such as board members, investors, contractors, suppliers and volunteers.

Policy elements

Information that iTech considers confidential and proprietary is undisclosed, valuable, expensive and/or easily replicated. More specifically, information that is classified as confidential includes but is not limited to:

- Customer lists (existing and prospective)
- Data of Customers/Partners/Vendors
- Trade secrets
- Private deals
- Unpublished financial information
- Processes, methods and know-how
- Patents, formulas or new technologies
- Pricing/marketing and other undisclosed strategies or tactics
- Unpublished goals, forecasts or initiatives that are marked as confidential
- Data entrusted to the company by external parties
- Documents, processes or other elements explicitly marked as confidential
- Any other knowledge acquired by employees during their employment

All these types of information must be protected for different reasons – some may be legally binding (e.g. sensitive data) and some constitute the backbone of the business and give it a competitive advantage (e.g. business processes). The disclosure of some kinds of information may expose iTech and/or iTech's clients to increased risk such as specific trade secrets, while for others the result could be the loss of important partners or reputation.

In the course of their employment, employees will have various levels of authorized access to confidential information so as to conduct their business. When they do so, the following rules strictly apply:

- No amount of information will be disseminated to anyone outside of the organization
- The disclosure of information inside the organization will be limited to those with authorized access and legitimate reason to require that information
- The information will not be used for the personal benefit or profit of the employee or any other except the company
- The employee will have access only to the amount and type of information required for the completion of their job responsibilities and no more
- Employees must limit to a minimum the occasions when they take confidential information out of the office
- When perusing or sharing information through electronic means, all precautionary safety measures must be in effect
- Confidential information must not be left unattended or unlocked
- Unauthorized replication of information is prohibited
- All copies of confidential documents must be shredded when no longer needed
- Upon separation of employment all confidential information must be returned or deleted from the employee's electronic devices

iTech will take measures to ensure that confidential information is well protected. Those measures include but are not limited to:

- Electronic information will be encrypted
- Databases will be protected with all available security measures
- Paper documents will be safely stored and locked
- Authorization of access will be carefully controlled, usually by senior management
- Employees may need to sign non-compete and/or non-disclosure agreements (NDAs)

Confidential information as described above may occasionally have to be disclosed for legitimate reasons, e.g. upon request of a regulatory body or for business purposes. In such cases, a strict procedure must be followed that includes the explicit consent of parties involved (unless they are faced with criminal charges) and the disclosure of only relevant information and no more.

Upon any known instance of violation, disclosure, accessibility, breach or transfer of any data considered to be proprietary or confidential in nature to unauthorized personnel the employee should report such incident to company management immediately.

Disciplinary Consequences

iTech places great importance in this policy. Any non-conformity will bring about disciplinary and, possibly, legal action. The company is prepared to terminate any employee who willfully or regularly breaches the confidentiality guidelines for personal profit. Serious offenses such as theft of information, illegal disclosure of sensitive data etc. will be grounds for immediate for-cause dismissal and may also involve legal consequences.

Any unintentional breach of this policy will be thoroughly investigated and will be punished appropriately depending on its magnitude and seriousness.

This policy is binding even after separation of employment.

Any closely related policies may be references and hyperlinked [here](#).