



SUPPLIER CODE OF ETHICS AND BUSINESS CONDUCT

Effective February 2026



Table of Contents

1. Purpose and Scope	4
Our Commitment to Integrity	4
Supplier Responsibility	4
Making Ethical Decisions	4
Reporting Violations	4
No Retaliation	6
2. Lawful Business Practices – Compliance with Laws and Regulations	6
Compliance Risk Management	6
Relationships with Competitors/Antitrust Concerns	6
Anti-Bribery and Anti-Corruption	6
Lobbying	7
Political Contributions	7
Money Laundering	7
Accurate Financial Records	7
International and Government Trade Laws	8
Insider Trading	8
3. Acting with Integrity/Responsibilities to Customers and Business Partners	8
Conflict of Interest	8
Gifts, Entertainment, and Prevention of Inappropriate Profits	9
4. Protecting Company and Client Assets	10
Confidential Information	10
Intellectual Property	10
Company Assets	10
Records Management and Retention	10
Email, Internet, and Information Systems	11
Communicating with Third Parties or the Media Responsibility	11
Use of Social Media	11
5. Fair Market Conduct	11
Fair Competition and Antitrust Laws	11
6. Global and Government Business	11
Maintaining Appropriate Relationships with Governments	11



Import and Export Compliance 12

7. Our Workplace Responsibilities and Commitments 14

 Respect for Individuals and Those with Whom We Work 14

 Workplace Health and Safety 15

 Drugs and Alcohol 15

 Privacy 15

8. Corporate Responsibility 15

 Our Role as a Corporate Citizen 15

 Human Rights and Human Trafficking 16

 Philanthropic and Charitable Activities 16

 Environmental Stewardship 16

Questions and Additional Guidance 16



BELL TECHLOGIX SUPPLIER CODE OF ETHICS AND BUSINESS CONDUCT

1. Purpose and Scope

Our Commitment to Integrity

This Supplier Code of Ethics and Business Conduct (“Code”) sets forth Bell Techlogix, Inc.’s (“Bell Techlogix” or the “Company”) expectations for the ethical and legal conduct of its suppliers, vendors, contractors, subcontractors, and third-party business partners (collectively, “Suppliers”).

Bell Techlogix recognizes that Suppliers may operate under their own codes of conduct or ethical business standards. Where a Supplier maintains its own written code, policy, or compliance program that meets or exceeds the standards set forth in this Code, Bell Techlogix considers that an acceptable equivalent. Suppliers must provide Bell Techlogix with documentation of such standards upon request.

Bell Techlogix, in its discretion, may amend, supplement, and interpret this Code as appropriate to ensure a culture of legal compliance and ethical conduct. This Code does not constitute a contract between Bell Techlogix and any Supplier and does not alter or supersede the terms of any existing agreement between Bell Techlogix and a Supplier.

Supplier Responsibility

Legal compliance and ethical conduct are foundational to Bell Techlogix’s business relationships. Bell Techlogix encourages all Suppliers to observe both the letter and spirit of this Code and to promote its principles within their own organizations and supply chains. Suppliers are encouraged to report any suspected or actual violation of law or the standards set forth in this Code by any party involved in the Company’s business. Suppliers who become aware of such concerns are encouraged to cooperate in any review or investigation.

Nothing in this Code should be construed as restricting or limiting a Supplier’s ability to file a complaint directly with any authorized government agency, testify truthfully in any public forum, exercise any legally protected rights, or comply with any applicable law or valid order of a court of competent jurisdiction.

Making Ethical Decisions

Bell Techlogix encourages Suppliers to use good judgment and common sense to comply with the letter and the spirit of this Code, and to avoid even the appearance of improper behavior. While this Code addresses common legal and ethical issues that may arise, it cannot address every scenario. When making a business decision that may have legal or ethical implications, Suppliers should think through the issues and, if not specifically addressed, use this Code as a roadmap for making ethical decisions.

When in doubt, Suppliers are encouraged to seek guidance from Bell Techlogix.

Reporting Violations

Bell Techlogix values openness and honesty and relies on its Suppliers to ensure that everyone acting on its behalf conducts business with honesty, integrity, and respect for the law. **Suppliers are encouraged to report, in good faith, any violations or suspected violations of this Code or any laws or regulations.**

Bell Techlogix encourages Suppliers to speak up with concerns without fear of retaliation.



At any time, Suppliers may reach out to Bell Techlogix, as designated below, for additional assistance or questions relating to reporting mechanisms or to make a report.

Suppliers may utilize any of the reporting mechanisms below and there is no order a Supplier must follow. Unless otherwise specified, wherever this Code directs Suppliers to report concerns, seek guidance, or contact Bell Techlogix, Suppliers should use the reporting mechanisms described in this section.

- By email to ethics@belltechlogix.com;
- In writing to Bell Techlogix's Chief Legal Officer; or
- By reporting directly to applicable government agencies or regulatory authorities, as further described in the Governmental Entities section of this Code.

Governmental Entities

Suppliers also have the right to make reports to applicable federal or state regulators **directly at any time** (this includes communicating to, cooperating with, responding to any inquiry from or providing documents or testimony to any regulatory or investigatory agency or authority), including without limitation, the United States Securities and Exchange Commission (SEC), the United States Department of Justice, and any applicable federal or state trade or law enforcement agency.

Nothing in this Code is intended to prevent, restrict, limit, impede or otherwise interfere with the rights of any Supplier to:

- Provide truthful disclosures to or communicate with any US federal or state law enforcement agencies, administrative, regulatory or self-regulatory agency;
- File a charge or complaint or initiate an investigation with an applicable government agency;
- Make other disclosures that are protected under U.S. laws, including for example, to the extent applicable, reporting possible violations of law in accordance with Section 21F of the U.S. Securities Exchange Act of 1934 and related rules;
- Communicate with any government agency or otherwise participate in any investigation or proceeding that may be conducted by any government agency, including providing documents or other information, without notice to or permission by Bell Techlogix;
- Receive any award or bounty from the government for information provided to any government agency; or
- Engage in any other legally protected communications or disclosures, to the extent not otherwise prohibited by applicable law or any binding agreement between the Supplier and Bell Techlogix.

Regardless of the method a Supplier uses to report, or whether or not a Supplier chooses to be anonymous, concerns that are raised under this Code of Ethics and Business Conduct will be investigated. If a Supplier chooses to report anonymously, Suppliers are encouraged to provide as much detailed information as possible. Bell Techlogix may follow up with the reporting party where contact information has been provided.

Where a violation of the law, this Code, or Company policy is substantiated, Bell Techlogix will take appropriate corrective action.

Investigation of Compliance Concerns

Bell Techlogix takes all reports of potential violations seriously. Upon receipt of a report of a suspected violation of this Code, Company policy, or applicable law, Bell Techlogix will conduct a prompt and thorough investigation.



Corrective Action

Bell Techlogix is committed to consistent and fair enforcement of this Code. Suppliers found to have violated this Code, Company policies, or applicable laws may be subject to remedial measures and possible termination of the relationship. Following an investigation that substantiates a violation of this Code, Company policy, or applicable law, the Chief Legal Officer will determine the appropriate corrective action.

No Retaliation

As noted above, Bell Techlogix strictly prohibits retaliation against any person who reports, in good faith, a suspected or actual violation of law or this Code. Reporting “in good faith” means making a genuine attempt to provide honest and accurate information, even if the information proves to be unsubstantiated or mistaken.

Bell Techlogix also prohibits retaliation because of a Supplier’s or Supplier personnel’s participation in a Company investigation. Any party that engages in retaliation in violation of this Section will be subject to remedial action, including termination of the Supplier’s engagement with Bell Techlogix.

Bell Techlogix strictly prohibits any form of retribution against Suppliers who, in good faith, raise questions, report concerns, make complaints, or participate in investigations.

Bell Techlogix takes reports of violations of law or this Code very seriously. Suppliers that submit false reports or that provide false information in a Bell Techlogix investigation will be subject to remedial measures, up to and including termination of the Supplier’s engagement with Bell Techlogix.

2. Lawful Business Practices – Compliance with Laws and Regulations

Compliance Risk Management

Suppliers are expected to conduct periodic internal assessments of their compliance with this Code and applicable laws. Suppliers must promptly report to Bell Techlogix any material compliance gaps or emerging risks that come to their attention in connection with their work for Bell Techlogix. Upon request, Suppliers must cooperate with Bell Techlogix and provide documentation demonstrating compliance with this Code. Failure to report material compliance gaps constitutes a violation of this Code.

Relationships with Competitors/Antitrust Concerns

While Bell Techlogix is a passionate competitor, it conducts business ethically and follows all applicable antitrust laws to ensure free and fair competition in the marketplace. Bell Techlogix strives to compete fairly and is committed to complying with applicable laws, including antitrust laws covering the pricing, promotion, distribution, purchase and sale of its products, as well as its relationships between manufacturers, suppliers, distributors, retailers, customers and competitors. The antitrust laws of the United States and other countries are designed to preserve and protect competition. Agreements between competitors relating to prices or allocations of territories or customers are prohibited. To live up to the letter and spirit of these laws, certain topics must never be discussed between Bell Techlogix and its competitors.

Anti-Bribery and Anti-Corruption

Bell Techlogix competes for business based on the merits and quality of its services. Bribery or corruption will not be tolerated, wherever it conducts business and regardless of local practices. Suppliers shall comply (and require that their subcontractors comply) with all applicable anti-bribery and anti-corruption laws, rules, and regulations, including, without limitation, the U.S. Foreign Corrupt Practices Act of 1977, as amended, and the U.K. Bribery Act of 2010 (collectively, “Anti-Bribery Laws”).



Regardless of local practices, competition or the nature of a gift, Suppliers and all parties acting on Bell Techlogix's behalf are expected to avoid all activity that could constitute bribery or corruption or that could give the appearance of such. Suppliers must never make illegal payments to government officials of any country.

Suppliers should never, directly or indirectly through a third party, provide or accept anything of value, such as payments, gifts, hospitality or business courtesies, or offers of future employment or consideration of future employment by Bell Techlogix that could be perceived as a bribe to obtain or retain business, favorable treatment or an improper benefit for or from Bell Techlogix. This expectation applies with particular force to officials (and their family members) of governments, state-owned or controlled entities, political parties and public international organizations, including universities, as well as candidates for political office and political parties.

Additionally, Suppliers are expected to ensure that all payments and financial exchanges related to Bell Techlogix business are for legitimate business purposes and are properly documented.

Prior to any discussion with current government officials, inspectors and other third parties with whom Bell Techlogix works, Suppliers are encouraged to contact Bell Techlogix.

Lobbying

Suppliers and their personnel are prohibited from undertaking, on behalf of Bell Techlogix, any activities intended to influence elected officials to act, or refrain from acting, with respect to legislation or other policy decisions.

Political Contributions

Suppliers should not engage in political activities, make political contributions, or use Bell Techlogix's funds, assets, or facilities to support any cause, political candidate, or party on behalf of Bell Techlogix.

Money Laundering

Money laundering involves disguising financial assets so they can be used without detection of the illegal activity that produced them. Through money laundering, a criminal seeks to "wash" the proceeds derived from criminal activity and make the funds appear to come from a legal source. Bell Techlogix is committed to complying with all anti-money laundering and anti-terrorism laws throughout the world. Bell Techlogix only does business with reputable entities who are involved in legitimate business activities and whose funds are derived from legitimate sources.

In support of this commitment, Suppliers are expected to be vigilant for any indication of money laundering activity and to remain alert to signs of possible illegal activities. Red flags of money laundering may include but are not limited to:

- Requests for large cash payments or other unusual payment terms.
- Structuring or breaking down payments into smaller amounts.
- Fund transfers to or from countries or territories unrelated to the transaction.
- Fund transfers to or from personal accounts, or accounts unrelated and without a logical relationship to the involved parties.

Bell Techlogix will not be a party to any agreement or action, which violates the money laundering laws of the United States or any country where we or our suppliers conduct business.

Accurate Financial Records

Accurate financial records are essential to Bell Techlogix's integrity and legal compliance. Suppliers who interact with Bell Techlogix's financial processes are expected to maintain accurate records and to comply with applicable laws and any financial requirements set forth in their agreements with Bell Techlogix.



If Bell Techlogix learns that its records are necessary for an internal or external audit, investigation, government inquiry or litigation, Bell Techlogix will notify Suppliers when relevant records must be preserved. Suppliers should never destroy, alter, or attempt to conceal any records in their possession once notified of such a requirement.

International and Government Trade Laws

While Bell Techlogix primarily operates in the United States, Bell Techlogix conducts business globally and as such is governed by many dynamic and complex laws, rules and regulations around the world. Whenever Bell Techlogix conducts international business, Bell Techlogix abides by all applicable laws, including the laws of international trade and applicable trade sanctions, wherever Bell Techlogix conducts such business. Many countries have laws regulating international trade that involve imports, exports, free trade agreements, investments, international financial transactions, and/or other types of business dealings. Suppliers involved in moving goods or providing services across international borders on behalf of Bell Techlogix are expected to know and comply with the laws of countries in which Bell Techlogix conducts business and to provide accurate information to regulatory agencies.

Government contracts are very complex and are subject to numerous policies, laws and regulations. Suppliers working on government contracts on behalf of Bell Techlogix are expected to know and comply with the applicable contract requirements, including any required disclosures.

Insider Trading

In the course of providing services to Bell Techlogix, Suppliers may encounter or be exposed to information about Bell Techlogix or its clients — such as contract awards, strategic decisions, or financial developments — that is not available to the general public and that could be relevant to decisions about whether to buy or sell shares of stock.

Material nonpublic information, or “inside information,” is information about a company (including companies that do business with Bell Techlogix) that is not available to the public and would be important to an investor in deciding whether to purchase or sell the company’s securities. This practice, known as “insider trading,” is unethical and illegal. “Stock tipping,” which involves providing inside information to any third party so that they might benefit financially, also carries severe legal penalties, including fines and imprisonment. Suppliers should never make a stock trade based on information they suspect is material and nonpublic.

Suppliers who obtain material nonpublic information in the course of their work with Bell Techlogix are expected to handle such information in accordance with applicable securities laws and any confidentiality obligations set forth in their agreements with Bell Techlogix.

3. Acting with Integrity/Responsibilities to Customers and Business Partners

Conflict of Interest

Suppliers are expected to avoid actual or perceived conflicts of interest in the performance of their duties. Suppliers should ensure their personal, financial, or business interests do not compromise their objectivity or integrity in performing services for Bell Techlogix. Therefore, it is each Supplier’s responsibility to avoid any actual or perceived conflict of interest. A conflict of interest arises when a Supplier’s personal, financial, or business interests could compromise — or reasonably appear to compromise — the Supplier’s objectivity, independence, or integrity in performing services for or on behalf of Bell Techlogix. For purposes of this Code, “immediate family member” means a Supplier personnel’s spouse, domestic partner, parent, sibling, child, or grandparent, and the step- and in-law equivalents of each of the foregoing.

Conflicts of interest may include, but are not limited to:



- Business activities or engagements that conflict with, or materially compromise, the Supplier's obligations to Bell Techlogix;
- Receiving improper personal benefits (or benefits received by the Supplier personnel's family) as a result of the Supplier's relationship with Bell Techlogix;
- Receiving loans, or guarantees of obligations, from a competitor, customer, supplier or someone seeking to do business with Bell Techlogix;
- Providing services to Bell Techlogix's direct competitors in a manner that materially conflicts with the Supplier's obligations to Bell Techlogix or compromises Bell Techlogix's confidential information;
- Operating a business that directly competes with Bell Techlogix in a manner that creates a material conflict with the Supplier's engagement or obligations to Bell Techlogix;
- Using proprietary or confidential business information for personal gain or to Bell Techlogix's detriment;
- Owning a material or financial interest in a business that competes with, is doing business with, or is seeking to do business with Bell Techlogix, other than an ownership interest in publicly traded securities;
- Acquiring any interest or asset of any kind for the purpose of selling or leasing it to the Company;
- Purporting to commit Bell Techlogix's resources, name, or support to any outside activity or organization without Bell Techlogix's prior written authorization; or
- Directing or influencing procurement or engagement decisions in favor of entities in which the Supplier or Supplier personnel have an undisclosed personal or financial interest.

To assist Suppliers in identifying and avoiding conflicts of interest, some important guidelines are set forth below.

Outside Business Activities. Suppliers must avoid outside business activities or financial interests that could compromise their objectivity or integrity in performing services for Bell Techlogix, and must disclose to Bell Techlogix any such activities or interests that could reasonably appear to create a conflict with their obligations to Bell Techlogix.

Directorships. Supplier personnel who serve in board or leadership roles at organizations that compete with, or do business with, Bell Techlogix must promptly disclose such relationships to Bell Techlogix. Suppliers must ensure that any such relationships do not compromise their obligations to Bell Techlogix or the confidentiality of Bell Techlogix's information.

Personal Financial Interests. Suppliers and their personnel must avoid personal financial interests that could influence, or reasonably appear to influence, their objectivity in performing services for Bell Techlogix. Suppliers must disclose to Bell Techlogix any financial interest in organizations that compete with, or do business with, Bell Techlogix where such interest could affect the integrity of the Supplier's work.

Personal Relationships. Suppliers must disclose to Bell Techlogix any personal or family relationships that could create a conflict of interest in connection with the performance of services for Bell Techlogix. Suppliers must not leverage personal relationships in ways that compromise the integrity of business decisions or the Supplier's obligations to Bell Techlogix.

Suppliers are encouraged to proactively disclose any actual or potential conflict of interest that may exist between themselves (and their relatives) and Bell Techlogix. Transparency through full disclosure will go a long way to avoiding a conflict of interest or the appearance of a conflict.

Gifts, Entertainment, and Prevention of Inappropriate Profits

The practice of giving or receiving business gifts requires careful consideration. Before any gift is exchanged, Suppliers should ensure it is permitted under this Code and any applicable Bell Techlogix policies. Business meals, entertainment,



or token gifts should be exchanged only when intended and understood as simple business courtesies meant to further communications or goodwill. Suppliers should not offer or accept anything of value from any party that could be construed as an attempt to influence or induce business decisions in connection with their work for Bell Techlogix.

“Business gifts” do not include company-sponsored sales contests or incentive programs. The following guidelines are provided to assist Suppliers.

The exchange of modest gifts and entertainment should never compromise professional judgment or be used for the inappropriate exchange of profits. Bribes and kickbacks are strictly prohibited. A bribe is typically a payment made to influence a single, discrete decision. It can be a one-sided offer to corrupt an official’s behavior. A kickback is a specific type of bribe that implies an ongoing relationship. The payment is often a percentage of the transaction value and is “kicked back” to the person who facilitated the deal. For example, a contractor might pay a project manager 10% of every invoice the manager approves.

- Suppliers should decline any gifts or entertainment that could be viewed as an attempt to influence a business decision.
- Suppliers should not accept gifts of cash or cash equivalents.
- Gifts exchanged in connection with Bell Techlogix business should be of modest value (under \$100) and infrequent.
- Government clients have very strict rules, often prohibiting gifts entirely. Suppliers working with Bell Techlogix’s government clients should be aware of and comply with any such restrictions.

4. Protecting Company and Client Assets

Confidential Information

Protecting the confidential information of Bell Techlogix, its clients, and business partners is a fundamental responsibility. Suppliers are expected to comply with all confidentiality obligations set forth in their agreements with Bell Techlogix and to handle confidential information in accordance with the standards set forth in this Code.

Intellectual Property

Suppliers are expected to protect Bell Techlogix’s intellectual property and respect the intellectual property rights of others.

Respect for Third-Party IP: Suppliers are prohibited from the unauthorized use, copying, or illegal reproduction of copyrighted works, patents, trademarks, and other intellectual property of other companies.

Trade Secrets: Suppliers must not engage in the fraudulent or unethical acquisition of other companies’ trade secrets.

Company Assets

Suppliers who are granted access to Bell Techlogix systems, equipment, facilities, or other assets in connection with their engagement are expected to protect those assets from loss, damage, theft, waste, and improper use. Suppliers should not use Bell Techlogix assets for purposes outside the scope of their engagement with Bell Techlogix.

Records Management and Retention

Suppliers are expected to maintain accurate records related to their work for Bell Techlogix and to comply with applicable records management and retention requirements. Where Bell Techlogix or its clients have implemented records management and retention policies applicable to the Supplier’s engagement, Suppliers are expected to comply with those policies.



Suppliers are expected to preserve any records, both paper and electronic, relating to any actual or threatened litigation or investigation involving Bell Techlogix. Suppliers must not alter, delete, conceal, or destroy any records that are subject to a legal hold.

Email, Internet, and Information Systems

Suppliers who are granted access to Bell Techlogix systems, networks, or data in connection with their engagement are expected to use such access only for authorized business purposes. Bell Techlogix reserves the right to lawfully monitor its systems, networks, and data. Suppliers should not expect privacy when accessing or using Bell Techlogix systems or transmitting data to or from Bell Techlogix.

Suppliers are expected to protect the security of Bell Techlogix systems and data. Suppliers should not share Bell Techlogix credentials, access codes, or other authentication information with any unauthorized person. Suppliers should use only authorized, secure methods to access or transmit Bell Techlogix data and should comply with Bell Techlogix's IT security requirements as a condition of their engagement.

Communicating with Third Parties or the Media Responsibility

Suppliers are not authorized to speak on behalf of Bell Techlogix and must not represent themselves as doing so to any third party. Any inquiry from a third party—including reporters, journalists, or analysts—seeking a statement or comment on Bell Techlogix's behalf must be declined and referred to Bell Techlogix's Marketing Department.

Use of Social Media

Suppliers who reference their engagement with Bell Techlogix in any online communication must make clear that they are not authorized to speak for or on behalf of Bell Techlogix. Suppliers must not post confidential information about Bell Techlogix, its clients, or business partners in any online communication. Nothing in this Code restricts a Supplier's legally protected rights, including the right to disclose facts relating to claims of sexual harassment, testify truthfully in any public forum, or comply with applicable law or a valid court order or directive from an authorized government agency.

5. Fair Market Conduct

Fair Competition and Antitrust Laws

Bell Techlogix is committed to competing vigorously and fairly in compliance with all applicable antitrust and competition laws. For detailed guidance on prohibited conduct with competitors, including pricing discussions and market allocation, refer to Section 2 (Relationships with Competitors/Antitrust Concerns) of this Code.

Prohibited Agreements: Suppliers must never discuss or agree with competitors on pricing, bid-rigging, or dividing markets.

Unfair Competition: Suppliers should not make false or misleading statements about Bell Techlogix's competitors.

6. Global and Government Business

Maintaining Appropriate Relationships with Governments

Interacting with government entities and public officials requires the highest level of integrity. Suppliers are expected to comply with the U.S. Foreign Corrupt Practices Act (FCPA).

Suppliers must never offer, promise, or provide anything of value to any government official, directly or indirectly, to obtain an improper advantage.



Import and Export Compliance

Suppliers must comply with all applicable import and export control laws and regulations in connection with products and services provided to Bell Techlogix or its clients, including: (1) the Arms Export Control Act (22 U.S.C. §§ 2751–2799aa-2) and the International Traffic in Arms Regulations (22 C.F.R. Parts 120–130) (“ITAR”); (2) the Export Control Reform Act of 2018 (50 U.S.C. §§ 4801–4826) and the Export Administration Regulations (15 C.F.R. Parts 730–774) (“EAR”); (3) the International Emergency Economic Powers Act (50 U.S.C. §§ 1701–1708) (“IEEPA”); and (4) U.S. sanctions laws and regulations administered by the Office of Foreign Assets Control (31 C.F.R. Parts 500–599) (collectively, “Export and Sanctions Laws and Regulations”). Suppliers must determine and maintain applicable Export Control Classification Numbers (ECCNs) and all required export authorization documentation for all products and services they provide to Bell Techlogix or its clients, and must provide such documentation to Bell Techlogix upon written request. Suppliers who are U.S. entities engaged in the business of exporting or manufacturing Defense Articles or furnishing Defense Services must maintain registration with the Directorate of Defense Trade Controls (“DDTC”) as required by ITAR throughout their engagement with Bell Techlogix and must maintain an effective export and import compliance program in accordance with ITAR. Suppliers shall not re-transfer any export-controlled articles or information (including Technical Data or software) to any third party without first complying with all applicable Export and Sanctions Laws and Regulations; Suppliers must contact Bell Techlogix prior to any proposed re-transfer. Suppliers must not conduct business with prohibited parties or in violation of applicable U.S. trade embargoes and sanctions programs.

Export Control Classification

Suppliers must determine and maintain the applicable Export Control Classification Number (ECCN) for all hardware, software, and technology provided to Bell Techlogix or its clients, including any applicable license exception determinations. Suppliers must provide ECCN classifications and related export authorization documentation to Bell Techlogix upon written request and must promptly notify Bell Techlogix of any change to a product’s or service’s export classification.

Restricted Party Screening

Suppliers must screen all relevant transactions and counterparties against the U.S. Government’s Consolidated Screening List (available at <https://www.trade.gov/consolidated-screening-list>) and other applicable restricted party lists prior to and on an ongoing basis throughout the provision of products or services to Bell Techlogix or its clients. Suppliers must document all screening activities and retain screening records in accordance with the Recordkeeping section of this Code. Any potential match identified through screening must be immediately reported to the Supplier’s Bell Techlogix contact and must not proceed until resolved. Suppliers must promptly notify Bell Techlogix in writing if it becomes ineligible perform, including due to: debarment or suspension; designation as a Specially Designated National or denied party under U.S. or foreign sanctions laws; expiration or cancellation of ITAR registration; a potential violation of Export and Sanctions Laws and Regulations; or initiation or existence of a U.S. federal, state, or local government investigation that could affect performance.

Prohibition on Redistribution and Re-export

Suppliers must not facilitate, directly or indirectly, the redistribution or re-export of any Bell Techlogix products or services to any unauthorized third party. Any request from a third party for redistribution or re-export of Bell Techlogix products or services, or any indication that a party intends to do so, must be immediately reported to Bell Techlogix.

Embargoed Countries



Bell Techlogix is prohibited from doing business with comprehensively embargoed countries, which currently include Cuba, Iran, the Democratic People's Republic of Korea (North Korea), Syria, and the Crimea, Donetsk, and Luhansk regions of Ukraine. This list is subject to change based on U.S. government sanctions programs. Suppliers who become aware of potential business activities involving personnel located outside the United States should verify that the relevant countries are not embargoed and raise any concerns to Bell Techlogix. Through its technology vendors, Bell Techlogix implements technical controls to block IP addresses associated with embargoed countries on Company-owned devices and systems. Suppliers must not attempt to circumvent these technical controls.

Red Flags

Suppliers must be alert to red flags that may indicate potential export control violations or sanctions evasion.

Red Flag Indicators

The following are examples of red flags that may indicate potential export control violations or sanctions evasion. If any of these indicators are present, Suppliers must stop the transaction and report it to Bell Techlogix immediately:

- **Unusual Payment Methods** – Payment from a bank account in a country unrelated to the transaction, requests for cash payments, cryptocurrency, or payment through multiple intermediaries.
- **Corporate Vehicles** – Use of shell companies, newly formed entities, or complex corporate structures that obscure the ultimate beneficial owner.
- **High-Risk Jurisdictions** – Transactions involving countries or regions with elevated diversion risk, including countries bordering Russia or known transshipment points.
- **Declining Maintenance or Support** – Customer declines standard maintenance, training, or support services that would normally accompany the product.
- **Suspicious End-Use** – The stated end-use is inconsistent with the customer's business or the product's typical applications.
- **Lack of Transparency** – Customer is reluctant to provide information about end-users, end-use, or business operations.
- **Geo-IP Location Anomalies** – User access or requests originating from IP addresses in embargoed countries or high-risk jurisdictions.
- **Changes to Shipping or Delivery** – Last-minute changes to delivery addresses, requests to ship to freight forwarders, or unusual routing.
- **Personal Email Addresses** – Use of personal email accounts (Gmail, Yahoo, etc.) rather than corporate email for business transactions.
- **Residential Addresses** – Delivery to residential addresses for commercial or enterprise products. Example: An order is to be delivered to an apartment address.
- **Past Russia/Belarus Orders** – Customer has a history of orders shipped to or involving Russia or Belarus prior to current restrictions.
- **Inconsistent Customer/Partner Information** – Discrepancies between information provided by the customer and publicly available information.
- **Inconsistent Documentation** – Documents contain errors, inconsistencies, or appear altered.
- **Evasive Financial Transactions** – Structuring payments to avoid reporting thresholds, or payments that do not match the transaction value.
- **Rapid or Unexpected Changes in Volume** – Sudden, unexplained increases in order volume or frequency.



- **No Web Presence** – Customer has no website, social media presence, or other verifiable online footprint. Example: large enterprise with hundreds of employees has no website and no LinkedIn presence.
- **Complex Distribution Models** – Transactions involving multiple intermediaries, resellers, or distributors without clear business justification.

Suppliers who encounter any of these red flags must stop the transaction and report it to Bell Techlogix contact immediately.

Upon a true match determination from restricted party screening or identification of other transaction red flags that cannot be resolved, Supplier must take immediate action to: (i) terminate the business relationship with the affected party; (ii) suspend any further activities with such party; and (iii) revoke such party's access to any products, services, and subscriptions.

Reporting Suspected Violations

Suppliers who suspect, know, or have reason to believe that a product or service may be used for unauthorized activities, including diversion to embargoed countries or restricted parties, must immediately report the concern. Suppliers should report to Bell Techlogix immediately.

Prohibited Telecommunications Equipment and Services

Section 889 of the National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232), prohibits U.S. government contractors from procuring or using certain telecommunications equipment and services produced or provided by Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, Dahua Technology Company, and their respective subsidiaries and affiliates ("Prohibited Telecom Equipment"). Suppliers must not furnish to, or on behalf of, Bell Techlogix any goods or services that use or incorporate Prohibited Telecom Equipment.

Recordkeeping

Suppliers must maintain documentation under this Section 6 for a minimum of five (5) years from the date of creation or as otherwise required by applicable law.

7. Our Workplace Responsibilities and Commitments

Respect for Individuals and Those with Whom We Work

Bell Techlogix values diversity and inclusion and encourages Suppliers to share this commitment within their own organizations. Suppliers are expected to foster work environments that respect the dignity of all individuals and are welcoming of individual differences.

Bell Techlogix expects Suppliers to comply with all applicable equal employment opportunity and anti-discrimination laws. To the extent applicable and legally permitted, Suppliers shall, to the extent applicable and legally permitted, adhere to the requirements of 41 CFR 60-1.4(a), 60-300.5(a), and 60-741.5(a). These regulations prohibit discrimination against qualified individuals based on their status as protected veterans or individuals with disabilities and prohibit discrimination against all individuals based on their race, color, religion, sex, sexual orientation, gender identity, national origin, and for inquiring about, discussing, or disclosing compensation. Moreover, these regulations require that covered prime contractors and subcontractors take affirmative action to employ and advance in employment individuals without regard to race, color, religion, sex, sexual orientation, gender identity, national origin, disability, or veteran status. Suppliers are expected to maintain workplaces free from discrimination, harassment, and retaliation, including sexual harassment and harassment based on protected characteristics. Suppliers should prohibit conduct that creates



an intimidating, offensive, or hostile work environment. Such conduct can take many forms, including physical, spoken, or written actions or comments.

Suppliers who become aware of, or experience, discrimination or harassment in connection with their engagement with Bell Techlogix are encouraged to report such conduct to Bell Techlogix. Suppliers are also expected to maintain their own processes for addressing discrimination and harassment complaints within their organizations.

Suppliers with questions regarding Bell Techlogix's expectations with respect to equal opportunity and anti-harassment are encouraged to contact Bell Techlogix.

Workplace Health and Safety

Bell Techlogix expects Suppliers to maintain safe and healthy work environments in compliance with all applicable health and safety laws and regulations, and to identify and address workplace hazards and safety risks in a timely manner.

Suppliers are expected to comply with all applicable laws and regulations intended to promote a safe and healthy work environment, including those governing occupational health and safety.

Suppliers are required to report and address workplace injuries and accidents in accordance with applicable law and their internal policies.

Suppliers are expected to maintain zero-tolerance policies with respect to workplace violence and threats of violence within their own organizations. While performing services at Bell Techlogix facilities, Supplier personnel are required to comply with Bell Techlogix's security policies, including any prohibition on weapons on Bell Techlogix property, consistent with applicable law.

Drugs and Alcohol

Supplier personnel performing services for or on behalf of Bell Techlogix must do so free from the influence of any substance— including alcohol, illegal drugs, controlled substances, or misused prescription medication—that could impair job performance or create safety risks. Suppliers must maintain appropriate substance use policies within their own organizations and ensure their personnel comply with Bell Techlogix's requirements while performing services for Bell Techlogix.

Privacy

Suppliers are expected to protect the privacy of their personnel and any individuals whose personal data they process in connection with services provided to Bell Techlogix. Suppliers must comply with all applicable privacy laws governing the collection, use, storage, and disclosure of personal data. Suppliers should ensure that access to sensitive personal information is restricted to those with a legitimate business need. Suppliers should promptly report any unauthorized disclosure of personal data arising from or related to their engagement with Bell Techlogix to Bell Techlogix.

Bell Techlogix's privacy obligations in connection with Supplier engagements are governed by applicable law and any data processing terms set forth in the parties' agreements.

8. Corporate Responsibility

Our Role as a Corporate Citizen

Bell Techlogix recognizes its role as a corporate citizen and is committed to supporting the communities where it operates. Suppliers are encouraged to share this commitment within their own organizations and to support initiatives that benefit their communities.



Human Rights and Human Trafficking

Bell Techlogix respects human rights and engages in fair employment practices. Human rights are a core value at the heart of how Bell Techlogix conducts its business. Suppliers are encouraged to share this commitment within their own organizations.

Bell Techlogix believes every person should be treated with dignity and has embedded respect for human rights and fair labor practices into its business. Suppliers are expected to comply with all applicable labor laws and should not knowingly engage with sub-suppliers or other third parties who violate labor or human rights laws.

Bell Techlogix is committed to respecting the human rights and dignity of everyone, and we support international efforts to promote and protect human rights. It is the Company's policy to comply with all child labor laws.

Bell Techlogix strictly prohibits any form of forced or compulsory labor or human trafficking. Suppliers who become aware of any suspicion or evidence of human rights abuses should report such concerns to Bell Techlogix.

Philanthropic and Charitable Activities

Bell Techlogix strives to make a positive impact in the lives of others and the communities where its employees live, work, and serve through volunteer activities, charitable giving, and other initiatives. Any charitable activities or contributions made by Suppliers in connection with Bell Techlogix's name or on its behalf require prior written authorization from Bell Techlogix.

Environmental Stewardship

Bell Techlogix is committed to conducting its business in an environmentally responsible manner through practical initiatives like recycling, energy conservation, and promoting digital documents. Suppliers are encouraged to conduct their operations in an environmentally responsible manner.

Questions and Additional Guidance

Bell Techlogix encourages all Suppliers to review this Code in its entirety and to conduct their business in a manner consistent with the principles and expectations set forth herein.

Suppliers with questions or requests for clarification regarding this Code may contact Bell Techlogix at ethics@belltechlogix.com.

Last Updated: February 24, 2026