

DELLTechnologies
SUPPLIER PRINCIPLES

Last updated: August 2025

Contents

Introduction	3
Scope	3
1. Compliance with Laws, Regulations, and International Standards	3
ANTI-CORRUPTION	4
ANTITRUST AND COMPETITION LAWS	5
ARTIFICIAL INTELLIGENCE AND AUTOMATED SYSTEMS.....	5
CERTIFICATIONS	6
GOVERNMENT PROCUREMENT AND FUNDING LAWS AND REGULATIONS.....	6
PRIVACY AND PERSONAL DATA PROTECTION.....	7
RESPONSIBLE SOURCING	7
RESTRICTED SOURCES AND TECHNOLOGIES	9
SECURITY OF INFORMATION, PRODUCTS, AND SYSTEMS.....	9
TRADE COMPLIANCE.....	10
WORKING CONDITIONS, FORCED LABOR, AND HUMAN TRAFFICKING	10
2. Core Policy Commitments and Supplier Requirements.....	11
ACCESSIBILITY REQUIREMENTS	11
CONFLICTS OF INTEREST.....	11
ENVIRONMENTAL REQUIREMENTS	11
FINANCIAL INTEGRITY AND ACCURATE RECORD KEEPING	12
GIFTS AND HOSPITALITY.....	12
INCLUSIVE LANGUAGE.....	12
RESPONSIBLE BUSINESS ALLIANCE CODE OF CONDUCT (RBA CODE)	12
UTILIZATION OF SMALL BUSINESS CONCERNS AND SUPPLIER SOURCING REQUIREMENTS	12
3. Supplier Engagement, Capability Building, and Assessment Programs	12
BUSINESS CONTINUITY.....	13
CONTINUOUS IMPROVEMENT	13
ENSURING SUPPLIER SUITABILITY.....	13
QUARTERLY BUSINESS REVIEWS	13
SUPPLIER ONBOARDING REQUIREMENTS	14
TRANSPARENCY AND REPORTING.....	14
4. Reporting Suspected Violations.....	14

Introduction

Dell Technologies, on behalf of itself and its direct and indirect subsidiaries (“**Dell Technologies**”), is committed to responsible business practices and ethical behavior. This includes holding our suppliers to the same high standards of excellence to which we adhere, as set forth in [Dell Technologies' Code of Conduct](#), and as articulated in governing laws and regulations, recognized international standards and conventions, and global best practices. Complying with Dell Technologies Supplier Principles (Principles) is a condition of doing business with Dell Technologies.

Scope

The Principles are applicable to Dell Technologies’ suppliers, including but not limited to final assembly, direct, indirect and sub-tier suppliers working within Dell Technologies’ supply chain, including suppliers’ workers, contractors, agents, and independent contractors, and sub-tier suppliers working within suppliers’ supply chain (“**Supplier(s)**”). Supplier compliance with the Principles is mandatory, and it is also mandatory for Key Suppliers (as defined below) to participate in Dell Technologies’ Supplier Engagement, Capability Building, and Assessment Programs (Section 3, below). For purposes of the Principles, covered workers of Suppliers include direct employees, temporary workers, migrant workers, student workers, contract workers, and any other person(s) providing labor and employment services to Supplier.

In cases of a Supplier’s non-compliance, Dell Technologies reserves the right to take all available legal actions and remedies for violations of the Principles, including without limitation the termination or reduction of business, onsite compliance auditing at Supplier’s expense, compensation and/or reimbursement to affected workers at Supplier’s expense, seeking of damages, and/or termination of Dell Technologies’ agreements with the Supplier.

1. Compliance with Laws, Regulations, and International Standards

Suppliers must comply with (a) all applicable laws, regulations and purchasing requirements (b) Dell Technologies policies, and (c) all applicable industry standards as outlined below.

(a) Applicable laws, regulations, and purchasing requirements include but are not limited to:

- Prevention of forced labor and respect for human rights and decent working conditions in supply chains, including, but not limited to, the United Kingdom (UK), Canada and Australian Modern Slavery Acts, the California Transparency in Supply Chains Act, Section 307 of the United States (U.S.) Tariff Act of 1930, the Uyghur Forced Labor Prevention Act (UFLPA) and the German Supply Chain Due Diligence Act (LkSG) (as applicable to each Supplier).
- Sanctions and export controls issued by regulators in applicable jurisdictions, including but not limited to the U.S. Treasury Department’s Office of Foreign Assets Control (OFAC), U.S. Commerce Department’s Bureau of Industry & Security (BIS), His Majesty’s Treasury of the United Kingdom, and the European Union (EU).
- Relevant government procurement and funding provisions including those under the U.S. Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation Supplement (DFARS) and any U.S. federal agency supplement.
- Anticorruption, Antitrust or competition designed or intended to prohibit, restrict or regulate actions having the purpose or effect of monopolization or restraint of trade.
- All applicable health, safety and environmental regulatory requirements.

(b) To demonstrate our commitment to a socially and environmentally responsible supply chain, we have established the following Dell Technologies' policies that all our Suppliers must adhere to:

- [Dell Technologies Human Rights Policy](#)
- [Dell Technologies Responsible Sourcing Policy](#)
- [Dell Technologies Statement Against Modern Slavery, Human Trafficking, and Child Labor](#)
- [Dell Technologies Vulnerable Worker Policy](#)

(c) Suppliers must adhere to the following applicable international standards and industry standards, including, but not limited to, the following:

- United Nations (UN) Conventions, including UN Convention Against Corruption, UN Declaration of Human Rights, UN Convention on the Rights of the Child and UN Guiding Principles on Business and Human Rights.
- Relevant International Labor Organization (ILO) conventions, including the eleven fundamental conventions, and conventions 1, 102, 131 and 170.
- Relevant International Organization for Standardization (ISO) management systems, including, but not limited to, ISO 9001 (Quality Management Standard), ISO 14001 (Environmental Management Standard), ISO 45001 (Occupational Health and Safety Management Standard), and ISO 50001 (Energy Management Standard).
- National Institute of Standards and Technology (NIST) Cybersecurity Framework.

All Suppliers are expected to conduct at least annual due diligence of their respective supply chains, which includes the use of risk assessments and mechanisms to objectively measure compliance by the Suppliers and their direct and indirect suppliers across their sub-tiers.

Dell Technologies uses its own assessment mechanisms to assess Supplier participation in Dell Technologies' Supplier Engagement, Capability Building and Assessment Programs, and engages with Suppliers to drive compliance and create shared value. Suppliers are also encouraged to highlight any risks or inability to adhere to any of the aforementioned laws, regulations, policies, or standards, as a part of doing business with Dell Technologies.

ANTI-CORRUPTION

Dell Technologies does not tolerate bribes, kickbacks, or extortion of any kind. Our zero-tolerance position on bribery is critical to uplifting the communities most impacted by corruption. Business decisions involving Dell Technologies shall always be made based on the merits of Dell Technologies' products and services.

Suppliers must comply with all applicable anti-bribery, anti-kickback, and anti-corruption laws and guidance, including without limitation, the U.S. Foreign Corrupt Practices Act, the UK Bribery Act, the UN Convention Against Corruption, and those in effect in jurisdictions where Suppliers act or purchase, market, sell, distribute, source, license, or deliver Dell Technologies' products or services ("Anti-Corruption Laws").

Suppliers must never offer, promise, request, authorize or accept a bribe, directly or through a third party, for any reason. A bribe can be anything of value, including cash payments, gifts, travel or lodging expenses, charitable donations, event sponsorships, meals, entertainment, or job opportunities, that is intended to improperly induce, influence, secure, or reward a decision or act of the recipient to promote the business interests of Dell Technologies.

Suppliers shall maintain and enforce reasonably adequate policies, procedures, and internal controls to ensure that Suppliers, and any person to whom Suppliers subcontract the provision of any element of the

services to be provided or who provides any services or receives any payment in connection with Suppliers' performance of services, comply with Anti-Corruption Laws. Suppliers agree to fully cooperate with Dell Technologies in the evaluation of program effectiveness.

Suppliers must conduct appropriate risk-based due diligence on any third party that Suppliers may contract, oversee, manage, transact with, direct, or otherwise engage in the context of Dell Technologies business, and to use such third parties only when necessary. Suppliers must not work with any individual or entity that engages in, or is suspected of engaging in, bribes, kickbacks, fraud, or other improper activities.

ANTITRUST AND COMPETITION LAWS

Dell Technologies is committed to free and fair competition. We work within the framework of applicable antitrust or competition laws ("Competition Laws"). Competition Laws mean any regulation designed to prohibit, restrict or regulate actions having the purpose or effect of restraining trade and lessening competition. Such conduct may include, but is not limited to, price fixing, market or customer allocation, bid rigging, or group boycott. The penalties for failing to comply with these laws can be severe and include significant fines and possible jail time for certain infractions. Violations may be proved by circumstantial evidence, including the inappropriate sharing of competitively sensitive information, such as pricing, customer information, tenders, cost information, forward-looking business plans or strategies. Competitively sensitive information is any information capable of affecting market behavior, including information relating to, for example: pricing or elements of pricing; markets or customers; production or output supply; potential bids or tenders; costs or elements of cost; Suppliers, contractors, or contract terms; intentions or forecasts regarding any of these; and other commercial strategies or plans.

We expect our Suppliers to comply with all relevant Competition Laws, including adopting relevant policies, processes and training, to ensure compliance with Competition Laws globally.

ARTIFICIAL INTELLIGENCE AND AUTOMATED SYSTEMS

Dell Technologies expects its Suppliers to use Artificial Intelligence and machine learning (AI) in a responsible, ethical, and legally compliant manner. AI tools, applications or systems developed or used in the provision of products or services to Dell Technologies must comply with applicable laws, regulations and industry best practices (e.g. the EU Artificial Intelligence Act), and Suppliers shall have all the rights and licenses in such AI tools, applications or systems that are necessary to allow Dell Technologies to use Supplier's products or services without additional restrictions .

Suppliers must maintain an inventory of and disclose upon request their use of AI tools, large language models, or systems that materially impact the design, development, delivery, support, or security of any product or service provided to Dell Technologies. Suppliers must not deploy AI systems that infringe intellectual property or privacy rights, result in unlawful profiling or discrimination, or otherwise present an unacceptable risk (as defined by regulation) to Dell Technologies, Dell Technologies' customers, or individuals. The use of any AI tools or systems in the provision of products or services to Dell Technologies must be subject to appropriate safeguards.

Upon request by Dell Technologies, Supplier shall provide a list of all AI tools, large language models, applications or system used in the provision of products or services to Dell Technologies identifying such AI technologies and describing the nature and purpose of such use.

Suppliers will implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the AI being utilized. Dell Technologies' data may not be incorporated in or used

to train any AI models or algorithms or any of Suppliers' AI systems or tools without the express written consent of Dell Technologies.

Suppliers must ensure AI systems used to process personal data comply with all applicable data protection laws and do not interfere with the exercise of individual rights. AI tools and systems must include human oversight where required and demonstrate transparency, fairness, and accountability. Suppliers shall cooperate with Dell Technologies in its AI governance and risk management reviews and provide relevant technical or compliance documentation upon request.

CERTIFICATIONS

All Suppliers engaged in the manufacturing and/or assembly of Dell Technologies-branded finished products shall achieve and maintain certification on the ISO Standards identified in the *Compliance with Laws, Regulations and International Standards* section, above. Suppliers who have certifications to similar standards or who are working to obtain initial certification must submit the alternate certificate or a certification schedule, respectively, to Dell Technologies for approval.

GOVERNMENT PROCUREMENT AND FUNDING LAWS AND REGULATIONS

Supplier's products or services may be used by Dell Technologies in fulfilling a government prime contract or subcontract or other government-funded contract requiring compliance with various procurement or funding laws and regulations, and socioeconomic programs. Therefore, Supplier is subject to these requirements in the applicable locations in effect at the time Dell Technologies issues its order, including but not limited to the United States Code of Federal Regulations ("CFR") at 48 CFR 52.211-15; all applicable clauses listed at 48 CFR 52.212-5(e) and 48 CFR 52.244-6; 2 CFR Part 200; 29 CFR Part 471, Appendix A to Subpart A; and 41 CFR 60-1.4(a), 60-300.5(a) and 60-741.5(a), which 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, or national origin. ***It is Supplier's responsibility to stay up to date on the list of clauses in 48 CFR 52.212-5(e) and 48 CFR 52.244-6, which are accessible at <https://www.acquisition.gov>.***

Supplier shall also comply with the provisions of 48 CFR 52.204-21, 48 CFR 252.204-7012, 48 CFR 252.204-7019, 48 CFR 252.204-7020, and 48 CFR 252.204-7021 if: (i) Supplier's performance involves access to "Federal contract information" or "covered defense information" (as those terms are defined in 48 CFR 52.204-21(a) and 48 CFR 252.204-7012(a), respectively); and (ii) Supplier is providing other than "commercially available off-the-shelf (COTS)" items (as defined in 48 CFR 2.101). If Supplier provides cloud services, Supplier shall comply with 48 CFR 252.239-7010.

By doing business with Dell Technologies, Supplier further represents that (i) neither it nor any of its principals are presently debarred, suspended, proposed for debarment, or declared ineligible for the award of contracts by any government agency; and (ii) it is providing current, accurate, and complete information when Dell Technologies relies on such information for representations to its customers, including, but not limited to, information, such as country-of-origin or place of manufacture, Supplier size or minority status, export classification, citizenship of relevant Supplier personnel, locations of relevant Supplier activities, compliance with applicable laws and regulations, and product certifications and standards or capabilities. Supplier shall immediately notify Dell Technologies of any relevant change in status of any of these representations.

To comply with laws and regulations governing supplier payment terms, Dell Technologies may request Suppliers provide documentation that they meet U.S. government criteria to be considered a small business and/or that business ownership has been certified by a Dell-recognized third-party certifying body. Should

size or ownership status change, Dell Technologies reserves the right to adjust payment terms back to our standard terms.

PRIVACY AND PERSONAL DATA PROTECTION

Dell Technologies expects its Suppliers to understand, track, and comply with all laws and regulations related to privacy and data protection that are relevant to their actions as a Supplier. Among other things, this means that Suppliers should access, collect, use, share, transfer or store the personal information of others only when specifically authorized, only as necessary for legitimate business purposes, and only to collect personal information of others with appropriate notices of the purposes for which that personal information will be used. Suppliers must meet the limitation of use requirements set forth in their Supplier agreement for any personal data received from Dell Technologies. As also required in Supplier agreements, Dell Technologies expects Suppliers to implement appropriate safeguards to ensure the protection, integrity, and security of personal information in accordance with applicable data privacy laws, including but not limited to the EU General Data Protection Regulation (GDPR), the UK Data Protection Act, the California Consumer Privacy Act (as amended by the CPRA), China's Personal Information Protection Law (PIPL), India's Digital Personal Data Protection Act (DPDP), and other applicable national or regional privacy laws. This includes holding accountable subcontractors that handle personal data to at least the same requirements imposed upon Suppliers. Dell Technologies also expects Suppliers to notify Dell Technologies promptly according to the terms of the Suppliers' agreement should a suspected or actual breach of data security occur with respect to personal data received from Dell Technologies or collected on behalf or for the benefit of Dell Technologies.

Suppliers are further expected to implement privacy-by-design and privacy-by-default principles for any systems, software, or services used to process personal data on behalf of Dell Technologies. Suppliers must maintain procedures for secure deletion and appropriate retention of personal data in accordance with applicable legal and contractual requirements, and ensure that such data is not used to train artificial intelligence or machine learning models without Dell Technologies' prior written authorization. Furthermore, Suppliers must assist Dell Technologies in responding to data-subject requests related to personal data they handle on behalf of Dell Technologies. This assistance includes, but is not limited to, providing necessary information, executing necessary actions, and ensuring that any subcontractors involved in processing the personal data also comply with these requirements. Suppliers are expected to comply with the timelines and procedures set forth by Dell Technologies for handling such requests to ensure compliance with applicable data privacy laws.

RESPONSIBLE SOURCING

Dell Technologies is committed to the responsible sourcing of materials used in our products and expects its Suppliers to adhere to the same high standards, which includes Dell's obligation to comply with the U.S. Dodd-Frank Act Section 1502, other responsible sourcing risks and applicable regulatory requirements, and all other applicable laws and regulations regarding the prevention of forced labor within our supply chain including but not limited to the UFLPA and 48 CFR 252.225-7060 (Prohibition on Certain Procurements from the Xinjiang Uyghur Autonomous Region).

Suppliers shall ensure compliance with Trade Compliance Laws (as defined below), including but not limited to the U.S. prohibition against importing goods produced in whole or in part with the use of convicted labor, forced labor, or indentured labor under the threat of penal sanctions (collectively, "forced labor"). Upon Dell's written request, Suppliers shall certify that forced labor was not employed in any stage of manufacture of the merchandise or any component or material thereof and that Suppliers do not purchase or otherwise obtain (directly or indirectly) any inputs (e.g., raw materials or intermediate components) used to produce the goods sold to Dell Technologies from any entities (a) located in a country, region, territory, or location subject to import restrictions enforced by U.S. Customs and Border Protection ("CBP") or any customs

authority of any other relevant jurisdictions; or (b) subject to CBP's or any customs authority of any other relevant jurisdictions' import restrictions.

Suppliers shall promptly provide all information to Dell Technologies with respect to the direct and indirect providers of the inputs (i.e., including upstream Suppliers and their direct and indirect suppliers across their sub-tiers.) used to produce the goods upon request from Dell, including, but not limited to, purchase orders, invoices, bills of lading, transportation documents, importation documents, raw material sourcing documentation, and pictures of raw materials, among others.

Suppliers shall promptly notify Dell Technologies of any detention activity directly or indirectly impacting Dell's goods and promptly respond to any Dell Technologies due diligence inquiries or requests for information made by Dell Technologies to ensure the compliance of the goods with CBP or other customs authorities' requirements. Suppliers shall provide full and timely cooperation regarding any requests from Dell Technologies and/or customs or regulatory authorities in relevant jurisdictions, promptly furnishing any information that may be reasonably required in the event of disclosure requests, or forced labor-related detentions, seizures, or enforcement actions initiated by the applicable authority. Furthermore, Suppliers must undertake all essential and judicious measures, including the timely submission of all necessary and appropriate reports, documents, and other materials to ensure compliance with the applicable laws.

Suppliers shall have a policy to assure that products manufactured with any mineral or materials identified as "conflict" or otherwise designated as requiring specific assurance (such as presenting a high risk of being produced with forced labor as defined under applicable laws) and incorporated in Dell Technologies-branded finished products do not directly or indirectly finance or benefit groups that engage in human rights violations in conflict-affected and high-risk areas, including but not limited to the Democratic Republic of the Congo or an adjoining country, region, territory, or location.

Such minerals, materials, and products include, but are not limited to, tantalum, tin, tungsten, and gold (3TG), lithium, nickel, natural graphite, cobalt, and mica. The list of such minerals, materials, and products might vary based on risk profiles and the use of such minerals within Dell Technologies-branded finished products supply chain.

Suppliers shall also conduct a supply chain survey to identify smelters and refiners of minerals, including 3TG, cobalt, lithium, mica, natural graphite, and/or nickel, within their supply chain, and report to Dell Technologies using the latest version of industry tools, including the Responsible Mineral Initiative's Conflict Minerals Reporting Template (CMRT) and the Extended Minerals Reporting Template (EMRT). Suppliers shall respond to Dell Technologies' requests for additional information or action that is necessary for Dell Technologies to complete its own due diligence as set forth in the OECD Due Diligence Guidance for Responsible Supply Chains from Conflict-Affected and High-Risk Areas and in the U.S. Dodd-Frank Act Section 1502, forced labor laws, or other responsible sourcing risks or applicable regulatory requirements.

Suppliers are expected to source from smelters or refiners (SORs) that are compliant with the Responsible Minerals Assurance Process (RMAP), London Bullion Market Association (LBMA) Good Delivery List, Responsible Jewellery Council (RJC), or equivalent certifications. In doing so, Suppliers should extend this expectation to their sub-tier Suppliers and take the necessary actions to remove from their supply chain SORs that are not participating in any reputable third-party assurance program, either through alternative sourcing or driving smelter certification. In the event of a non-compliant approved third-party audited SOR being reported, Supplier shall provide a mitigation plan to expedite the non-compliant SOR's removal or resolution at the same time as reporting non-compliance conformance in accordance with RMAP, RJC, LBMA, or equivalent certifications. Notwithstanding the foregoing, Dell reserves the right, in its sole discretion, to request the removal of an SOR that Dell determines is non-compliant based upon Dell's reasonable due diligence standards.

RESTRICTED SOURCES AND TECHNOLOGIES

Supplier represents that it does not provide: (1) covered telecommunications equipment or services, or (2) any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The following terms: “covered telecommunications equipment or services”, “substantial or essential component”, and “critical technology” are as defined in 48 CFR 52.204-25 or by any United States Executive Order. Supplier also represents that it does not provide to Dell Technologies any products, solutions, software, or technologies (or any substantial/essential component thereof) that are sourced from any person or provider that is restricted as a source by the FAR. Supplier shall immediately notify Dell Technologies directly if it sources from any Supplier restricted by the FAR.

SECURITY OF INFORMATION, PRODUCTS, AND SYSTEMS

Dell Technologies expects its Suppliers, and their subcontractors, to maintain a security and risk management program aligned with industry standards and applicable laws, to identify and mitigate security risks that could negatively impact the information, data, assets, products, systems or networks of Dell Technologies or its customers. Suppliers, including their subcontractors, must implement administrative, technical, and physical controls that align with industry frameworks (e.g., ISO 27001, NIST Cybersecurity Framework) and cover, at a minimum: program governance, access management, secure software development, vulnerability management, network security, incident response, Human Resources (HR) security, training, and physical security. Access to Dell information, data, systems, assets, networks, facilities, products and/or the information, data, systems, assets, networks or facilities of Dell customers (Dell Systems) is subject to the terms of the Supplier Agreement and requires an approved non-disclosure agreement.

Suppliers must conduct security awareness training (and/or undergo Dell's third-party Security Awareness Training) for its personnel, including employees and contractors, at least annually. Clear security roles and responsibilities must be defined for Supplier's employees, contractors, and third-party users; consequences for non-compliance with security policies should be communicated. To the extent permissible under law, Supplier shall conduct background investigations (in accordance with the Dell Standards, available at [Candidate Guidelines Notice of Convictions](#)) of all of Supplier's workforce who perform services for or have access (logical or physical) to Dell Systems and/or Dell customers. Supplier shall prohibit the performance of any services under the Supplier Agreement and/or access to the Dell Systems by any individuals who have been found to have engaged in criminal acts that involve fraud, dishonesty, or breach of trust or that constitute a felony under applicable law.

Suppliers are responsible for ensuring security compliance and validation for security controls at least as comprehensive as set forth herein. Facilities and systems connecting to Dell Systems, or storing or processing information or data on Dell Systems must be adequately secured with appropriate physical and information security measures. Supplier must establish access control policies, including requiring unique user IDs and strong password practices, regularly reviewing access to applications and data, and revoking access when no longer required. Applications, services, and access points not necessary for business functionality should be disabled or removed. Supplier shall meet Dell Technologies availability requirements for provided applications, follow secure development practices, apply security patches and updates in a timely manner and conduct code reviews for product releases, as applicable. Supplier shall use detection, prevention, and recovery controls to protect Dell Systems against malicious software and its vulnerability remediation efforts should be tracked, monitored, and verified. Suppliers must establish a documented information security event management process; incident response, escalation, and remediation procedures should be in place, and shall notify Dell of any security incidents involving Dell Systems within 24 hours of detection at Security@Dell.com.

Supplier shall implement and maintain counterfeit mitigation measures that substantially meet the system criteria specified in 48 CFR 252.246-7007 (Contractor Counterfeit Electronic Part Detection and Avoidance System); provide to Dell Technologies on request, information concerning such counterfeit mitigation measures; and address any material deficiencies in such mitigation measures that may be identified by Dell Technologies or by Supplier. Unless the Supplier is the “original manufacturer” (as defined by 48 CFR 252.246-7008), Supplier shall also comply with 48 CFR 252.246-7008 (Sources of Electronic Parts).

Key Suppliers that operate in the capacity of Dell’s Original Design Manufacturers (ODM) and Contract Manufacturers (CM), and applicable ODM and/or CM Suppliers, that Dell Technologies buys from directly and/or provide substantial product transformation as listed on the Public Supplier List ([dell-suppliers.pdf](#)) (Key Suppliers), shall also adhere to Dell Technologies’ security standards and requirements, as applicable.

TRADE COMPLIANCE

Suppliers shall comply with export control and economic sanctions laws and regulations of the United States, the European Union, United Kingdom, and all applicable jurisdictions (Trade Compliance Laws). This includes, without limitation, export licensing requirements, end-user, end-use, and end-destination restrictions, prohibitions on dealings with sanctioned individuals and entities, including, but not limited to, persons on the U.S. Office of Foreign Assets Control’s (OFAC) Specially Designated Nationals and Blocked Persons List, or the U.S. Department of Commerce Denied Persons List, Bureau of Information and Security (BIS) Entity List, Military End-User List, and Military Intelligence End-User List, as amended, entities otherwise subject to military end-use restrictions, as well as the UFLPA Entity List. Export or re-export to Russia or Belarus or for use in Russia or Belarus are expressly prohibited. Dell Technologies reserves all rights and remedies to enforce this restriction, including injunctive relief, damages, and cancellation/termination of Dell Technologies’ agreement(s) with the Supplier. Suppliers agree not to violate the Trade Compliance Laws with respect to sourcing, licensing, or delivery of products to Dell Technologies. Suppliers shall maintain trade compliance policies and procedures, including screening procedures that are adequate to ensure that Suppliers comply with the Trade Compliance Laws.

WORKING CONDITIONS, FORCED LABOR, AND HUMAN TRAFFICKING

Dell Technologies is committed to respecting the human rights of workers at any tier of its supply chain, and to treating them with dignity and respect. Workers include direct employees, temporary workers, migrant workers, student workers, contract workers, and any other person(s) providing labor and employment services to a Supplier. In addition to the international standards listed in the Statement of Principles, this commitment also encompasses (but is not limited to) the following core tenets:

- Forced, bonded (including debt bondage) or indentured labor, involuntary prison labor, slavery or trafficking of persons of any age shall not be used, including prohibiting the use of recruitment fees by Suppliers or labor agents recruiting workers.
- No misleading or fraudulent practices by employers or labor agents during worker recruitment.
- Child labor is prohibited.
- Compliance with 48 CFR 52.222-50 (Combating Trafficking in Persons).

These and additional requirements are aligned with the international frameworks listed in the *Compliance with Laws, Regulations and International Standards* section, above.

2. Core Policy Commitments and Supplier Requirements

Dell Technologies imposes specific requirements on its Suppliers with respect to the following issue areas:

ACCESSIBILITY REQUIREMENTS

Suppliers and all Supplier services and deliverables that Supplier provides to Dell must comply with applicable accessibility requirements, including but not limited to: the [Americans with Disabilities Act \(ADA\) of 1990](#), [Section 508 of the Rehabilitation Act of 1973](#), [Accessible Canada Act \(ACA\)](#), [European Accessibility Act \(EAA\)](#), [21st Century Communications and Video Accessibility Act \(CVAA\)](#) and all other applicable global laws and standards. All Suppliers providing deliverables or services and relating to web content or web functionality must meet the [Web Content Accessibility Guidelines \(WCAG\) version 2.2, Level AA](#). Suppliers are responsible for and must implement accessibility into any device, product, website, web-based application, cloud service, software, software output, mobile application, marketing material, or content developed or provided by or on behalf of Supplier to Dell Technologies or its customers. Supplier must address accessibility issues identified, at no additional cost to Dell. Remediation must be based on the severity of the issue. Furthermore, Suppliers need to provide Dell access to accessibility findings and updates (via vendor portal, Jira tracking or other applicable platform, regular meetings, etc.) and should test and validate their products a minimum of annually, and/or remediate accessibility findings. When the digital asset is software, application, or hardware, the supplier needs to provide a [Voluntary Product Accessibility Template](#) showing the level of accessibility. Suppliers must perform and deliver according to the Dell policies expressed by the [Accessibility Statement](#). Failure to meet the standards and requirements may result in harm to Dell, and delays or cancellation of payment to Supplier, etc.

CONFLICTS OF INTEREST

Suppliers must avoid both actual and potential conflicts of interest involving Dell Technologies' business. A conflict of interest consists of any circumstance, including a personal relationship, the giving or receiving of lavish business courtesies, a business investment, or other financial interest that may compromise a Supplier's ability to act with objectivity and in the best interests of Dell Technologies. Suppliers shall not conduct Dell Technologies business with a Dell Technologies employee who has a romantic, familial, or other personal relationship with a current employee of their company. Suppliers must promptly disclose to Dell Technologies all pertinent details of any personal, financial, or other situation that represents or appears to represent an actual or potential conflict of interest.

ENVIRONMENTAL REQUIREMENTS

As part of our goal to reduce the environmental impact of our operations, Dell Technologies is working with Suppliers in Dell's Emissions Supplier Engagement Program (ESEP) to reduce their total scopes 1, 2 and upstream scope 3 greenhouse gas (GHG) emissions by 45%, compared to 2019 levels, by 2030. In line with the Responsible Business Alliance Code of Conduct v.8.0, all Dell suppliers are encouraged to establish and report against an absolute corporate-wide greenhouse gas reduction goal; track, document, and publicly report energy consumption and all Scopes 1, 2, and significant categories of Scope 3 GHG emissions; and look for methods to improve energy efficiency and to minimize their energy consumption and greenhouse gas emissions.

Dell Technologies' Suppliers are encouraged to share water data, monitor water use and implement water management and water risk mitigation plans to achieve reductions in water use and wastewater discharge.

Dell Technologies requests all final assembly and component material Suppliers to achieve third-party certification to a nationally adopted version of ISO 50001.

FINANCIAL INTEGRITY AND ACCURATE RECORD KEEPING

Suppliers must maintain and provide, upon request, proper, accurate, complete, and reliable financial and business records to Dell Technologies relating to any transactions or expenditures relevant to any Dell Technologies business. Suppliers are prohibited from “parking funds”, creating “slush funds”, or engaging in similar improper or false accounting practices.

GIFTS AND HOSPITALITY

All gifts, meals, travel, or entertainment offered or provided by Suppliers must comply with Anti-Corruption Laws, in addition to other applicable laws, rules, regulations, and policies. Gifts or hospitality shall never be offered or provided under circumstances that are improper or create the appearance of impropriety.

Suppliers are prohibited from offering or providing gifts greater than 100 United States Dollar (USD) (or equivalent in local currency) or lavish hospitality to Dell Technologies’ team members.

INCLUSIVE LANGUAGE

Dell Technologies is committed to the use of inclusive language in our products and across our supply chain. Using language that helps capture individuals of all backgrounds and experiences with our Suppliers, with our customers, and with our team members is an important step in cultivating a welcoming culture. We are remediating non-inclusive language over time where practicable and preventing future ongoing use. Suppliers should avoid the use of non-inclusive terms in code and content within deliverables provided to Dell Technologies.

RESPONSIBLE BUSINESS ALLIANCE CODE OF CONDUCT (RBA CODE)

Dell Technologies is proud to be a founding and full member of the RBA. [The Responsible Business Alliance Code of Conduct](#) establishes standards for safe, responsible, ethical, and sustainable business operations in which workers are treated with respect and dignity. Dell Technologies has fully adopted the RBA Code of Conduct, including, but not limited to, its standards and audit procedures, and expects facilities managed by its Suppliers to abide by the most recently updated RBA Code and for them to expect the same of their Suppliers. Dell Technologies manages its own facilities to the same standards.

UTILIZATION OF SMALL BUSINESS CONCERNS AND SUPPLIER SOURCING REQUIREMENTS

Suppliers must (1) comply with all applicable laws and regulations, including, but not limited to, 48 CFR 52.219-8 (Utilization of Small Business Concerns), (2) take proactive efforts to ensure that subcontracting processes are conducted in a manner that promotes opportunity for qualified businesses of all backgrounds to participate in Supplier’s supply chain, (3) maintain accurate records of Supplier’s efforts under this provision; and (4) submit quarterly reports to Dell Technologies on request, including with respect to Supplier’s spend with small and other businesses.

3. Supplier Engagement, Capability Building, and Assessment Programs

To help ensure that global standards and Dell Technologies policy commitments are implemented and reinforced, Dell Technologies requires Key Suppliers to participate in its programs to understand and evaluate risks and Supplier performance, build capability to meet and exceed applicable standards, and address areas of concern.

Programs include, but are not limited to, managing working hours, maintenance of management systems, ensuring onsite health and safety standards, environmental reporting and disposition of electronic material.

Suppliers are identified for programs according to Dell Technologies' own assessment mechanism and are expected to participate as requested. In addition to these programs, Suppliers are expected to immediately report any incident, which encompass any of the conditions listed below which result in the following:

- Death;
- Significant injury to three or more employees or injury to 10 or more employees;
- Any infectious disease outbreaks such as Coronavirus Disease (COVID-19), Severe Acute Respiratory Syndrome (SARS), tuberculosis, or public health events required by [International Health Regulations](#) to be reported to the World Health Organization;
- Environmental pollution that has been cited or acknowledged by local government;
- Environmental, safety or human rights-related issue reported by public media or a non-governmental organization (NGO);
- Environmental, health, safety, or other related issue resulting in a relocation or shutdown notice from local government;
- Environmental, health, safety, or other related issue resulting in relocation or shutdown planning or roadmaps by a Supplier; or
- Fire or other safety incidents causing significant property loss.

BUSINESS CONTINUITY

Dell Technologies' global footprint, flexibility, and Suppliers' relationships are key to the resilience of our supply chain. Dell Technologies expects Suppliers to develop and maintain a business continuity and resiliency plan (BCRP) in accordance with Supplier's agreement with Dell Technologies. Suppliers may also be asked to provide information regarding business continuity preparedness, as aligned with ISO 22301.

CONTINUOUS IMPROVEMENT

Dell Technologies is committed to responsible sourcing and Suppliers must meet the standards specified in the Principles. With a focus on self-assessment, internal ownership and self-accountability, Suppliers should continue to make changes that will bring long-lasting, sustainable impact not only to their own facilities and operations, but also to Dell Technologies.

ENSURING SUPPLIER SUITABILITY

Dell Technologies conducts appropriate risk-based due diligence on all Suppliers during the initiation of the relationship, and throughout the term of the relationship. Suppliers must comply with Dell Technologies' due diligence procedures and provide complete, accurate, and timely information when requested to facilitate such efforts.

In addition, Suppliers must provide periodic certifications of Suppliers' compliance with relevant laws and the Principles, and perform any other requested mitigation activities, in a form, manner and timeframe acceptable to Dell Technologies.

QUARTERLY BUSINESS REVIEWS

As solely determined by Dell, certain Suppliers must undergo a quarterly business review with Dell Technologies, which includes scoring and/or metrics, as determined by Dell Technologies, of their supply chain performance aligned to the Principles, particularly regarding sustainability, risk, security, safety and environment. Dell Technologies Suppliers are evaluated quarterly and should expect their scores to influence Dell Technologies' purchasing decisions.

SUPPLIER ONBOARDING REQUIREMENTS

As part of Dell Technologies' due diligence and risk management processes, Suppliers must complete onboarding through Dell Technologies' designated supplier engagement platforms, which may include tools such as Aravo, OneTrust, or other systems as specified by Dell Technologies. Suppliers shall provide accurate and complete information through these tools in the form, manner, and timeframe specified, and shall maintain current and up-to-date records throughout the duration of the relationship. Failure to comply with onboarding requirements may result in delays or denials of payment, delays in engagement, or termination of the supplier relationship.

TRANSPARENCY AND REPORTING

Transparency is important to Dell Technologies' customers and other stakeholders. To this end, Dell Technologies publicly discloses certain assurance information. This information includes, but is not limited to, annually aggregated data on Dell Technologies' social and environmental responsibility programs and a list of Dell Technologies' Key Suppliers.

If Suppliers become aware of facts or circumstances that will likely lead to or cause violations/misconduct of the Principles, the Suppliers must immediately notify Dell Technologies. In the event Dell Technologies receives substantive allegations of violations/misconduct, Dell Technologies reserves the right to immediately investigate the allegations and if required by law, will disclose all relevant information related to the allegations to the appropriate authorities.

When requested, suppliers must provide data required for ecolabel certifications. Suppliers acknowledge that Dell may provide the supplier data to conformity assurance bodies and the data may be disclosed publicly, as required.

Dell Technologies encourages Suppliers to participate in environmental reporting. Suppliers must also provide information about social and environmental responsibility, including compliance with Dell Technologies policies, when requested by Dell Technologies or when required by applicable law.

4. Reporting Suspected Violations

Speak Up: Your Voice Matters! It is important to immediately report suspected violations of the Supplier Principles. Dell Technologies will not retaliate against anyone who provides information or otherwise assists in an investigation or proceeding regarding any conduct the person reasonably believes constitutes a violation of applicable laws, regulations, or the Principles. Suppliers are expected, consistent with applicable laws and contractual obligations, to provide reasonable assistance to any investigation by Dell Technologies of a violation of the Principles or applicable laws and allow Dell Technologies reasonable access to all facilities, records, and documentation concerning their compliance with the Principles and laws applicable to Dell Technologies' procurement of Supplier's products and/or services.

If Suppliers know of, or suspect, a violation of applicable laws or regulations or the Principles, or human rights, working conditions or environmental concerns, Suppliers are encouraged to utilize the following reporting options:

- Dell Technologies' Speak Up tool at <https://dell.service-now.com/arc>.
- Audit Committee of the Dell Technologies Board of Directors at Board_of_Directors@dell.com.
- Dell Technologies' Privacy team at Privacy@dell.com for matters involving personal information.

Any reported violation will be kept confidential to the maximum extent allowed under applicable laws. Such reports may be made anonymously, by using any of the methods set forth above. Although reports of

violations or suspected violations under the Principles may be made verbally, Suppliers are encouraged to make any such reports in writing, which assists the investigation process.