



## Dell Supplier Principles

(Revision March 2021)

### Introduction

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

### Scope

These Principles are applicable to final assembly, direct and sub-tier suppliers working within Dell’s supply chain, including suppliers’ employees, contractors, agents, independent contractors, and sub-tier suppliers within suppliers’ supply chain (“Supplier(s)”). Supplier compliance with these Principles, as well as participation in Dell’s Supplier Engagement, Capability Building and Assessment Programs as further outlined below, is mandatory.

In cases of non compliance, Dell reserves the right to take any and all available actions against Suppliers for violations of these policies, including without limitation the termination or reduction of business, frequent required onsite compliance auditing at Supplier’s expense, employee compensation at Supplier’s expense, seeking of damages, and/or termination of Dell’s agreement with the Supplier.

### Statement of Principles

Dell’s Suppliers must comply with:

- All applicable laws, regulations, and purchasing requirements, including but not limited to relevant provisions under the US Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation Supplement (DFARS) and any U.S. federal agency supplement.
- [Dell Human Rights and Labor Policy](#).
- [Dell Responsible Sourcing Policy](#)
- [Dell Vulnerable Worker Policy](#)
- [Dell Slavery and Human Trafficking Policy Statement](#)
- The Responsible Business Alliance (RBA) [Code of Conduct](#)
- United Nations (U.N.) Conventions, including U.N. Declaration of Human Rights, U.N. Convention on the Rights of the Child and U.N. Guiding Principles on Business and Human Rights.
- UK and Australian Modern Slavery Acts.
- California Transparency in Supply Chains Act.
- Relevant International Labor Organization (ILO) conventions, including the eight fundamental conventions and conventions 1, 102, 131, 155 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 Standard), ISO 27001 (Information Security Standard), and ISO 22301 (Business Continuity Management Standard).
- NIST (National Institute of Standards and Technology) Cybersecurity Framework.



Suppliers shall meet these Principles through three (3) primary means:

- Meet or exceed applicable laws and recognized international standards;
- Ensure compliance with Dell's aforementioned Statement of Principles; and
- Actively participate in Dell's Supplier Engagement, Capability Building and Assessment Programs.

All Suppliers are expected to conduct at least annually due diligence of their respective supply chains, which includes the use of risk assessments and mechanisms to objectively measure compliance. Dell uses its own assessment mechanisms to scope Supplier participation in Dell's 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 adhering to these standards as a part of doing business with Dell.

## 1. Compliance with Laws, Regulations and International Standards

### COMPLIANCE WITH LAWS AND REGULATIONS

It is essential to a socially and environmentally responsible supply chain that Suppliers conduct its business legally, and ethically. Dell and Suppliers shall comply with all applicable laws and regulations.

### TRADE COMPLIANCE

Suppliers shall comply with export control and economic sanctions laws and regulations. of the United States, the European Union and other 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 and Entity Lists, as amended, as well as entities subject to military end-use restrictions. Supplier agrees not to violate the Trade Compliance Laws with respect to sourcing, licensing or delivery of products to Dell. Supplier shall maintain trade compliance policies and procedures that are adequate to ensure that Supplier complies with the Trade Compliance Laws.

### ANTI-CORRUPTION

Dell does not tolerate bribes, kickbacks or extortion of any kind. Business decisions involving Dell shall always be made based on the merits of Dell products and services.

Suppliers must comply with all applicable anti-bribery, anti-kickback, and anti-corruption laws, including without limitation, the U.S. Foreign Corrupt Practices Act, the United Kingdom Bribery Act of 2010, and those in effect in jurisdictions where Suppliers act or purchase, market, sell, distribute, source, license, or deliver Dell 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.

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 the Anti-Corruption Laws. Suppliers agree to fully cooperate with Dell in the evaluation of program effectiveness.

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

#### GIFTS AND HOSPITALITY

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

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

#### FINANCIAL INTEGRITY AND ACCURATE RECORD KEEPING

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

#### PRIVACY AND PERSONAL DATA PROTECTION

Dell 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. As also required in Supplier agreements, Dell expects Suppliers to implement appropriate safeguards to ensure the protection, integrity, and security of personal information in accordance with applicable data privacy laws. This includes holding accountable subcontractors that handle personal data to at least the same requirements imposed upon the Supplier. Dell also expects Suppliers to notify Dell promptly according to the terms of the Supplier's agreement should a suspected or actual breach of data security occur with respect to personal data received from Dell or collected on behalf or for the benefit of Dell.

#### PROTECT CONFIDENTIAL AND PROPRIETARY INFORMATION

Dell respects the importance of privacy to its customers, employees and other individuals as a fundamental human right, and integral to Dell maintaining their trust. Accordingly, Dell expects its Suppliers to understand, track, and comply with all laws and regulations globally 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, store or dispose ("Process") of the personal data of others only when and as specifically authorized by Dell, only as necessary for legitimate business purposes, and only in accordance with appropriate notices and/or consents applicable to the collection of such personal data. Suppliers must meet the limitation of use and all other processing requirements set forth in their Supplier agreement for any personal data received from Dell. As also required in Supplier agreements, Dell expects



Suppliers to implement appropriate safeguards to appropriately protect the confidentiality, integrity, and availability of personal data in accordance with applicable data privacy and information security laws, regulations, and any applicable regulatory and industry standards. This includes requiring subcontractors that Process personal data to uphold at least the same requirements imposed upon the Supplier, and holding them accountable for such requirements. Dell also expects Suppliers to notify Dell promptly according to the terms of the Supplier's agreement should a suspected or actual breach of data security occur with respect to personal data received from Dell or collected on behalf or for the benefit of Dell.

#### COMPLY WITH ANTITRUST AND COMPETITION LAWS

Dell is committed to observing the applicable antitrust or competition laws ("Competition Laws") of all countries in which it conducts business and expects Suppliers to share that commitment. The Competition Laws prohibit actions which are deemed to unreasonably restrain trade, such as, but not limited to, fixing prices or allocating customers. The penalties for failing to comply with these laws can be severe and include significant fines and possible jail time for certain infractions.

#### CERTIFICATIONS

All Suppliers engaged in the manufacturing and/or assembly of Dell-branded finished products shall achieve and maintain certification on the ISO Standards identified in the Statement of Principles, 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 for approval.

## 2. Core Policy Commitments and Supplier Requirements

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

#### RESPONSIBLE BUSINESS ALLIANCE (RBA) CODE OF CONDUCT

Dell is proud to be a founding member of RBA. The RBA Code of Conduct ("Code") establishes standards for safe, responsible, ethical and sustainable business operations in which workers are treated with respect and dignity. Dell expects facilities managed by its suppliers to abide by the Code and for them to expect the same of their Suppliers; in doing so, Dell manages its own facilities to the same standards.

#### FEDERAL ACQUISITION REGULATION (FAR)

If Dell is providing Supplier's products or services under a United States government prime contract or subcontract, Supplier shall comply with the applicable provisions of the Federal Acquisition Regulation, published in the version of Title 48 of the United States Code of Federal Regulations ("CFR") at 52.244-6 in effect on the date Dell issues its order to Supplier. ***It is Supplier's responsibility to stay up-to-date on the list of clauses in 52.244-6***, but the clauses in effect as of the date of these Principles are: 52.203-13 (Contractor Code of Business Ethics and Conduct); 52.203-15 (Whistle-blower Protections Under the American Recovery and Reinvestment Act of 2009); 52.203-19 (Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements); 52.204-21 (Basic Safeguarding of Covered Contractor Information Systems); 52.204-23 (Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities); 52.204-25 (Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment); 52.219-8 (Utilization of Small Business Concerns); 52.222-21 (Prohibition of Segregated Facilities); 52.222-26 (Equal Opportunity); 52.222-35 (Equal Opportunity for Veterans); 52.222-36 (Affirmative Action for Workers with Disabilities); 52.222-37 (Employment Reports on Veterans); 52.222-40 (Notification of Employee Rights Under the National Labor Relations Act); 52.222-50 (Combating Trafficking in Persons); 52.222-55



(Minimum Wages under Executive Order 13658); 52.222-62 (Paid Sick Leave Under Executive Order 13706); 52.224-3 (Privacy Training); 52.225-26 (Contractors Performing Private Security Functions Outside the United States); 52.232-40 (Providing Accelerated Payments to Small Business Subcontractors) and 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels. Suppliers shall also comply with the requirements of 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.

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(a) and 48 CFR 252.204-7012(a), respectively); and (ii) Supplier is providing other than Commercial Off-The-Shelf items. Dell may require Supplier to separately certify its compliance with any of the above cited regulations.

#### 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 terms "covered telecommunications equipment or services," "substantial or essential component," and "critical technology" are as defined in FAR 52.204-25 or by any United States Executive Order. Supplier also represents that it does not provide to Dell 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 FAR. Supplier shall immediately notify Dell directly if it sources from any supplier restricted by FAR.

#### WORKING CONDITIONS, FORCED LABOR AND HUMAN TRAFFICKING

Dell is committed to upholding 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 Supplier. In addition to the international standards listed in 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 at any tier of the supply chain, including use of recruitment fees by suppliers or labor agents recruiting workers.
- No misleading or fraudulent practices by employers or labor agents during employee recruitment.
- Child labor is prohibited in any tier of the supply chain.

These and additional requirements are aligned with the international frameworks listed in Statement of Principles, above.

#### MINERALS AND EXTRACTIVES

Dell is committed to the responsible sourcing of materials used in our products and expects its Suppliers to adhere to the same high standards.



Suppliers shall have a policy to assure that products manufactured with mineral identified as “conflict” or otherwise designated as requiring specific assurance, and incorporated in Dell-branded finished products do not directly or indirectly finance or benefit armed groups that engage in human rights violations in the Democratic Republic of the Congo or an adjoining country.

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

Suppliers shall also conduct a supply chain survey to identify smelters and refiners of minerals, including 3TG and/or cobalt within their supply chain, and report to Dell using the last version of industry tools, including the Responsible Mineral Initiative’s Conflict Minerals Reporting Template (CMRT). Suppliers shall respond to Dell’s requests for additional information or action that is necessary for Dell to complete its own due diligence as set forth in the U.S. Dodd-Frank Act, Section 1502 or other responsible sourcing risks or applicable regulatory requirements.

Suppliers are expected to source from smelters and refiners that are compliant with the Responsible Minerals Assurance Process (RMAP). In doing so, Suppliers should extend this expectation to their third party suppliers and take the necessary actions to remove non-compliant or non-active smelters from their supply chain, either through alternative sourcing or driving smelter re-certification. In the event of a non-compliant RMAP smelter being reported, Dell expects a mitigation plan to expedite the non-compliant smelter’s removal or resolution at the same time as reporting non-compliances.

#### SUPPLY CHAIN SECURITY

Dell takes a holistic and multifaceted approach to protecting its supply chain and delivering solutions that customers can trust. This includes multiple layers of controls across the supply chain ecosystem and following and driving international risk management standards and best practices. Suppliers are expected to maintain security controls and risk management processes to identify and mitigate sourcing, cyber, and physical security risks throughout the product lifecycle and provide product integrity.

Suppliers must (1) 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); (2) provide to Dell on request, information concerning such counterfeit mitigation measures; and (3) address any material deficiencies in such mitigation measures that may be identified by Dell or by Suppliers. Suppliers must also adhere to existing Dell security policies as applicable, including, but not limited to, data protection agreements, secure development specifications, and logistics security.

Suppliers are encouraged to drive security best practices aligned to industry standards such as ISO 27001 and NIST Cybersecurity Framework, among others, and collaborate with Dell on continuous improvement.

#### SUPPLIER DIVERSITY

Dell believes an ethical, diverse supply chain is a vital part of its business. Suppliers must meet the following diversity requirements: (1) comply with any applicable law and regulation targeted towards Suppliers to governmental entities; (2) use reasonable efforts to engage minority-owned businesses, women-owned businesses, small businesses, LGBT-owned businesses and disabled-owned businesses if Supplier engages subcontractors to provide any deliverables or to support the Supplier’s overall business operations; (3) use commercially reasonable efforts to engage small businesses as defined by the United States Small Business Administration (including small business subcategories such as small disadvantaged businesses, small women-owned businesses, veteran-owned businesses, service disabled



veteran-owned businesses and HUB zone businesses) if Supplier engages subcontractors in the United States to provide any deliverables or to support the Supplier's general business operations; (4) maintain accurate records of Supplier's efforts under this provision; and (5) report to Dell on request, Supplier's spend with minority-owned businesses, women-owned businesses, small businesses, LGBT-owned businesses and disabled-owned businesses.

#### AVOID CONFLICTS OF INTEREST

Suppliers must avoid both actual and potential conflicts of interest involving Dell 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. Suppliers shall not conduct Dell business with a Dell employee who has a romantic, familial, or other personal relationship with a current employee of their company. Suppliers must promptly disclose to Dell all pertinent details of any personal, financial, or other situation that represents or appears to represent an actual or potential conflict of interest.

#### USE OF INCLUSIVE LANGUAGE

Dell is committed to the use of inclusive language in our products and across our supply chain. We are remediating non-inclusive language over time where practicable and preventing future ongoing use. Suppliers should avoid use of non-inclusive terms in code and content within deliverables provided to Dell, with sensitivity to terms such as:

- Master/Slave or Master-Slave
- Slave
- Master
- Blacklist/Whitelist or Blacklist-Whitelist
- Blacklist, Black list
- Whitelist, White list
- Blackhat, Black hat
- Whitehat, White hat
- Segregate/Segregation
- Blackout
- Man-hour, man day
- Manpower
- Rule of Thumb

### 3. Supplier Engagement, Capability Building and Assessment Programs

To help ensure that global standards and Dell policy commitments are implemented and reinforced, Dell requires Suppliers to participate in its programs to understand and evaluate risks and Supplier performance, build capability to meet and exceed applicable standards, and remedy 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; disposition of electronic material. Suppliers are identified for programs according to Dell's own assessment mechanism and are expected to participate as requested. In addition to these programs, Suppliers are expected to 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 labor issue reported by public media or 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.

#### ENSURING SUPPLIER SUITABILITY

Dell 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's due diligence procedures and provide complete, accurate, and timely information where requested to facilitate such efforts.

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

#### BUSINESS CONTINUITY

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

#### QUARTERLY BUSINESS REVIEWS

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

#### AUDIT RIGHTS

Dell may audit Supplier, upon notice and in a non-disruptive fashion, to ensure compliance with Applicable Laws, the Agreement and the Supplier Principles.

#### TRANSPARENCY AND REPORTING

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

If Suppliers become aware of facts or circumstances that will likely lead to or cause violations/misconduct of these Principles, the Suppliers must immediately notify Dell. In the event Dell receives substantive allegations of violations/misconduct, Dell 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.





Unless exempted by Dell, Suppliers shall publish, at its own expense, (a) an annually updated public sustainability report based on the Global Reporting Initiative (GRI) or other internationally recognized framework and (b) participate in environmental reporting. Suppliers must also provide information about social and environmental responsibility, including compliance with Dell policies, when requested by Dell.

## CONTINUOUS IMPROVEMENT

Dell is committed to responsible sourcing and Suppliers must meet the standards specified in these 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.

### 4. Reporting Suspected Violations

If Suppliers know or suspect of a violation of applicable laws or regulations or these Principles, Suppliers are encouraged to report as follows:

- Contact Dell's Global Ethics and Compliance Office at [ethics@dell.com](mailto:ethics@dell.com);
- Contact the Audit Committee of the Dell Board of Directors at [Board\\_of\\_Directors@dell.com](mailto:Board_of_Directors@dell.com);
- Contact Dell's Ethics Helpline at [www.dell-ethicsline.com](http://www.dell-ethicsline.com);
- For matters involving personal information, contact Dell's Privacy team at [Privacy@dell.com](mailto:Privacy@dell.com).

Any reported violation will be kept confidential to the maximum extent allowed under applicable laws. Such reports may be made anonymously, where local law permits, by using any of the methods set forth above. Although reports of violations or suspected violations under these Principles may be made verbally, Suppliers are encouraged to make any such reports in writing, which assists the investigation process.

Dell 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 or these Principles.

Suppliers are expected, consistent with applicable laws and contractual obligations, to provide reasonable assistance to any investigation by Dell of a violation of these Principles or applicable laws, and to allow Dell reasonable access to all facilities, records and documentation concerning their compliance with these Principles and laws applicable to Dell's procurement of Supplier products and/or services.