# Microsoft Supplier Code of Conduct

Microsoft's mission is to empower every person and every organization on the planet to achieve more. Achieving our mission isn't just about building innovative technology. It's also about who we are as a company and as individuals, how we manage our business internally, and how we work with customers, partners, governments, communities, and suppliers.

Through the Standards of Business Conduct, Microsoft has established company standards that include ethical business practices and regulatory compliance. Similarly, Microsoft expects the companies with whom we do business to embrace this commitment to integrity by complying with—and training their employees on—the Microsoft Supplier Code of Conduct (SCoC).

## COMPLIANCE WITH THE SUPPLIER CODE OF CONDUCT

Suppliers and their employees, personnel, agents, and subcontractors (collectively referred to as "Suppliers") must adhere to this Supplier Code of Conduct while conducting business with or on behalf of Microsoft. Suppliers must require their subcontractors acknowledge and implement the SCoC in their operations and across their supply chains. Suppliers must promptly inform their Microsoft contact, a member of Microsoft management, or the contacts provided at the end of this document when any situation develops that causes the Supplier to operate in violation of this Code of Conduct.

All Microsoft Suppliers must conduct their employment practices in full compliance with all applicable laws and regulations and in compliance with Microsoft requirements, which may exceed local legal requirements. In all cases in which Microsoft requirements are more stringent than local legal requirements, Suppliers are required to meet the more stringent Microsoft requirements.

While Microsoft Suppliers are expected to self-monitor and demonstrate their compliance with the SCoC, Microsoft may audit Suppliers or inspect Suppliers' facilities to confirm compliance. Suppliers that behave in a manner that is unlawful or inconsistent with the SCoC, or any Microsoft policy, risk termination of their business relationship with Microsoft. Complying with the SCoC and completing the SCoC training provided by Microsoft are required in addition to meeting any other obligations contained in any contract a Supplier may have with Microsoft.

## LEGAL AND REGULATORY COMPLIANCE PRACTICES

All Microsoft Suppliers must conduct their business activities in full compliance with all applicable laws and regulations while conducting business with and/or on behalf of Microsoft, and must, without limitation, meet the following requirements:

**Trade**: Comply with all international laws, national laws, regulations, and other controls which govern the transfer, access, export, re-export, and import of products, services, and technology.

Suppliers must maintain, where applicable, robust compliance programs and policies to manage technologies, products, and technical data that is controlled or restricted by law.

Suppliers will not provide controlled technologies, products, or technical data to Microsoft, without providing notice of such controls as necessary for Microsoft to maintain compliance with applicable laws.

**Antitrust**: Conduct business in full compliance with antitrust and fair competition laws that govern the jurisdictions in which they conduct business.

**Boycotts**: Not participate in international boycotts which are not sanctioned by the United States (U.S.) Government.

**Anti-Corruption**: Conduct business in full compliance with the U.S. Foreign Corrupt Practices Act ("FCPA") and the anti-corruption and anti-money laundering laws that govern the jurisdictions in which Suppliers conduct business.

- Suppliers must comply with all applicable anti-corruption and anti-money laundering laws, including the FCPA, as well as laws governing lobbying, gifts, donations, hiring, and payments to public officials, political campaign contribution laws, and other related regulations. Suppliers must prohibit any and all forms of bribery, corruption, extortion, and embezzlement. All business dealings shall be transparently performed and accurately reflected in Supplier's business books and records. Compliance monitoring, record keeping, and enforcement procedures shall be implemented to ensure compliance with anti-corruption laws.
- No Supplier shall, directly or indirectly, promise, authorize, offer, or pay anything of value (including but not limited to gifts, travel, hospitality, charitable donations, or employment) to any government official or other party to improperly influence any act or decision of such official for the purpose of promoting the business interests of Microsoft in any respect, or to otherwise improperly promote the business interests of Microsoft in any respect.
- "Government official" refers to all of the following: (i) any employee of a government entity or subdivision, including elected officials; (ii) any private person acting on behalf of a government entity, even if just temporarily; (iii) officers and employees of companies that are owned or controlled by the government; (iv) candidates for political office; (v) political party officials; and (vi) officers, employees and representatives of public international organizations, such as the World Bank and United Nations.
- Suppliers must report signs of any personnel, representative, or partner performing unethically or engaged in bribery or kickbacks.
- As representatives of Microsoft, Suppliers must comply in all respects with Microsoft's Anti-Corruption Policy for Representatives.

**Accessibility**: Over one billion people around the world live with a broad range of disabilities including vision, hearing, mobility, cognitive, speech and mental health conditions. Creating products, apps, and services that are accessible to people of all abilities is part of our DNA at

Microsoft as well as our mission of empowering every person and organization on the planet to achieve more. Each Microsoft Supplier must comply with:

- The most recent version of the international accessibility standard Web Content Accessibility Guidelines (WCAG) Level A and AA when creating any deliverable; and
- All applicable Microsoft requirements and standards for creating accessible devices, products, websites, web-based applications, cloud services, software, mobile applications, content, or services.

## BUSINESS PRACTICES AND ETHICS

All Microsoft Suppliers must conduct business interactions and activities with integrity and trust, without limitation:

**Business Information Reporting:** All business information and reporting activities are to be conducted honestly and accurately and comply with all applicable laws regarding their completion and accuracy.

**Communication**: Be honest, direct, and truthful in discussions, including those with regulatory agency representatives and government officials.

**Press**: Only speak to the press on behalf of Microsoft if expressly authorized in writing to do so by a Microsoft communications representative.

**Publicity**: Suppliers will not issue press releases or other publicity related to their relationship or contracts with Microsoft without the prior written consent of the Microsoft contract signee.

**Gifts and Entertainment:** Use good judgment when exchanging business courtesies. Gifts, meals, entertainment, hospitality, and trips that are lavish or lack transparency or a legitimate purpose may be viewed as bribes, may create the appearance of a conflict of interest, or may be perceived as an attempt to improperly influence decision making. Giving business courtesies to Microsoft employees, if permitted at all, should be modest and infrequent. Never give anything to gain an improper business advantage. When deciding whether to give a gift, entertainment, or other courtesy, apply the following requirements:

- Suppliers are prohibited from paying expenses for travel, lodging, gifts, hospitality, entertainment, or charitable contributions for government officials on Microsoft's behalf.
- Travel expenses must be reasonable, have legitimate business purposes, and not be excessive or lavish. (See Travel section below.)
- Do not offer anything of value to obtain or retain a benefit or advantage for the giver, and do not offer anything that might appear to influence, compromise judgment, or obligate the Microsoft employee.
- Entertainment and meals should be modest, infrequent, and occur in the normal course of business.
- Suppliers may not offer any business courtesy unless it is permissible under both this Code and the Supplier's gift policy.

- Be aware of limits. The value of any courtesy offered by a Supplier to a Microsoft employee may not exceed the limits applicable to the employee's business unit and country. Microsoft business unit and country limits may prohibit courtesies entirely or set maximum limits at varying amounts. It is the Supplier's responsibility to ask the recipient what the applicable limits are and to not exceed those limits.
- Suppliers are not allowed to give gifts of any value to any member of Microsoft Procurement or its representatives.
- Any morale events for employees of the Supplier should be organized by the Supplier, and not by Microsoft. If employees of the Supplier need to participate in a morale event with Microsoft FTEs, Microsoft should work out a plan for shared funding with the Supplier.

**Conflicts of Interest**: Be honest, direct, and truthful when answering questions from Microsoft about relationships with Microsoft employees. Avoid improprieties and conflicts of interests or the appearance of either. Suppliers must not deal directly with any Microsoft employee whose spouse, domestic partner, other family member or relative holds a financial interest in the Supplier.

**Insider Trading**: Insider trading is prohibited. Under Federal Securities Laws you cannot buy or sell Microsoft or another company's securities when in possession of information about Microsoft or another company that is (1) not available to the investing public, and (2) could influence an investor's decision to buy or sell the security.

**Travel**: All Suppliers must comply with the Travel Guidelines for Suppliers.

**Engaging Subcontractors:** Obtain written consent from Microsoft prior to engaging a subcontractor to fulfill Supplier's obligations to Microsoft in addition to meeting any other obligations contained in any contract a Supplier may have with Microsoft.

## HUMAN RIGHTS AND FAIR LABOR PRACTICES

Microsoft expects its Suppliers to (1) comply fully with all employment laws, (2) share its commitment to respect all human rights and to provide equal opportunity in the workplace as set forth in the Universal Declaration of Human Rights, the UN Guiding Principles on Business and Human Rights, the UN Global Compact Principles and the ILO Core Labour Standards, and (3) take effective measures to remedy any adverse human rights and fair labor impacts, including the disclosure of any and all potential violations and cooperating fully in subsequent investigations into such violations. All Microsoft Suppliers must, without limitation:

- **Not discriminate and not harass.** Suppliers must commit to a workforce and workplace free of harassment, unlawful discrimination, and retaliation. Suppliers should ensure their business practices respect the rights of different demographic groups, including women, and migrant workers. While we recognize and respect cultural differences, Suppliers must provide equal opportunity in the workplace and reasonable accommodation, and not engage in harassment or discrimination

in employment on the basis of age, ancestry, citizenship, color, family or medical care leave, gender identity or expression, genetic information, immigration status, marital or family status, medical condition, national origin, physical or mental disability, political affiliation, union membership, protected veteran status, race, religion, sex (including pregnancy), sexual orientation, or any other characteristic protected by applicable local laws, regulations, and ordinances.

Supplier shall not require workers or potential workers to undergo medical tests including pregnancy tests, except where required by applicable laws or regulations or prudent for workplace safety and shall not improperly discriminate based on test results. Suppliers must accommodate all disabilities to the extent required by law.

- **Prohibit the use of child labor.** Child labor must not be used under any circumstance. Suppliers must not employ anyone under the age of 15, under the age for completing compulsory education, or under the legal minimum working age for employment, whichever requirement is most restrictive. Suppliers are required to have a remediation plan in place to ensure that, in the event of any child labor found, Suppliers must follow international standards, local legal requirements, or Microsoft's child labor remediation requirements. Microsoft supports all forms of legal youth employment, including the development of legitimate workplace apprenticeship programs for the educational benefit of young people. Microsoft will not do business with any Supplier that uses such programs in a fraudulent or deceptive manner. Suppliers must prohibit workers who are under the age of 18 from performing work that is likely to jeopardize their health or safety such as night work, overtime, heavy lifting and working with toxic or hazardous materials.
- **Prohibit the use of Forced Labor, Prison Labor and Trafficking in Persons.** All Suppliers, including recruiters, employment agencies, sub-agencies, and recruitment firms, are prohibited from using forced labor and prison labor, trafficking in persons, and the procurement of commercial sex acts. All forms of forced labor are prohibited, including indentured labor, bonded labor (including debt bondage, trafficked or slave) or any other form of forced labor. All forms of prison labor are prohibited. Support for or engagement in any form of human trafficking or involuntary labor through threat, force, fraudulent claims, or other coercion is prohibited. Suppliers must have a voluntary labor compliance plan in place that (1) provides provisions for training Supplier personnel and raising their awareness of issues related to forced labor, and (2) details what remediation the Supplier will provide in case of any violations. All Suppliers must inform employees, agents, sub-agencies, recruiters, contractors, and subcontractors about Supplier's policies that prohibit human trafficking, prison labor, forced labor, and other forms of slavery and provide training and programs to promote awareness, risk identification, employee reporting, corrective action, and potential penalties for violations.
- **Ensure workers have access to identity-related and personal documents.** Suppliers, agents, and sub-agents are prohibited from requiring workers to lodge "deposits," withholding employee identity or immigration papers (including but not limited to passports, drivers' licenses, or work permits (regardless of the issuing authority), or destroying, concealing, confiscating, or otherwise restricting or denying workers' access

to such documents. Workers must be free to resign their employment in accordance with local and national laws or regulations without unlawful penalty.

- **Provide safe housing when the Supplier intends to provide accommodations.** If the Supplier will provide housing or hotel accommodations for employees working in the country where work will be performed, all accommodations provided must be in compliance with the host country's housing and safety standards.
- **Provide return transportation for foreign migrant workers.** When hiring foreign workers who are not nationals of the country in which the work is taking place and who are recruited and who migrate from their home country to another country for the specific purpose of working for the Supplier, Suppliers must provide return transportation for such workers or reimburse the workers for the cost of such trip upon the end of their employment. This requirement does not apply to workers with permanent residency of professional employees who are on short-term or long-term assignments.
- **Use appropriately trained recruiters to support compliance.** Suppliers must use recruiters, employment agencies, and recruiting companies that are trained and which comply with international standards, local labor laws of the countries in which the recruitment takes place, or Microsoft requirements, whichever are stricter. Recruitment fees or other similar fees charged to workers and payable to the employer, recruiting agent, or sub-agent are strictly prohibited. If such fees are found to have been paid by workers, Suppliers will be required to repay such fees to the workers.
- **Make conditions of employment clear when hiring.** Suppliers must prohibit the use of misleading or fraudulent practices during the recruitment or employment process. Suppliers must disclose, in a format and language accessible to the worker, basic information regarding the key terms and conditions of employment, including wages and fringe benefits, the location of work, living conditions, housing and associated costs (if any), any other costs to be charged to the worker, and any hazards involved in the work. Such disclosures must be made before the worker enters employment and as needed throughout their term of employment. All contracts and employee handbooks (where applicable) must (1) clearly convey the conditions of employment in a language understood by the worker, and (2) reflect applicable laws and regulations.
- **Provide written employment contracts or agreements when necessary.** If required by law or contract, Suppliers must provide an employment contract, recruitment agreement or other work document in writing, in a language that the employee understands, that includes details about work descriptions, wages, prohibitions on charging recruitment fees, work locations, living accommodations and associated costs, time off, roundtrip transportation arrangements, grievance processes, and the content of applicable laws and regulations that prohibit trafficking in persons. If the employee must relocate to perform the work, the work document shall be provided to the employee at least five days prior to that relocation. Foreign migrant workers must receive the employment contract prior to the worker departing from his or her country of origin and there shall be no substitutions or changes to the employment contract upon arrival in

the receiving country unless changes are made to meet applicable law and/or provide equal or better employment terms.

- **Provide fair compensation.** Suppliers must provide fair compensation for all employees and workers, including employees who are permanent, temporary, or dispatched, migrant workers, apprentices, and contract workers. Such compensation must meet the legal minimum standards as required by local law. Workers with disabilities whose wages are governed by section 14(c) of the Fair Labor Standards Act must receive no less than the full minimum wage rate as defined by Executive Order 13658. All employees and workers shall be provided with a clear, timely, and understandable wage statement that includes sufficient information to verify accurate compensation for work performed. Suppliers may not use deductions from wages as a disciplinary measure. Any deductions from wages not provided for by national law or local law are permitted only with proof of express, written, and freely given permission of the worker concerned. All disciplinary measures must be recorded. Wages and benefits paid for a standard work week must meet local and national legal standards. Suppliers must provide benefits to employees that meet legal standards and at the levels expected in the industry and in accordance with Microsoft requirements.

- **Treat employees with dignity and respect.** Suppliers must not engage in any harsh or inhumane treatment, including violence, gender-based violence, sexual or other harassment including psychological harassments or threats, sexual abuse, corporal punishment, mental or physical coercion, bullying, or public shaming. Verbal abuse or other forms of intimidation are prohibited. Suppliers shall have a humane treatment policy and monitor supervisors to ensure appropriate conduct. Disciplinary policies and procedures in support of these requirements shall be clearly defined and communicated to workers.

- **Meet working hours and rest day requirements.** Suppliers are prohibited from requiring workers to work more than the maximum hours as set by international standards, including the International Labour Organization, around standard working hours (Conventions 1, 14, & 106), local and national laws, Microsoft requirements, or in the freely negotiated and legitimate collective agreement, whichever are most restrictive. Suppliers must ensure overtime is voluntary and paid in accordance with local and national laws or regulations. A work week must not be more than 60 hours per week, including overtime, except in emergency or unusual situations. Workers must be allowed at least one day off per seven-day work week. Suppliers must keep employee working hours and pay records in accordance with local and national laws or regulations and provide such records to Microsoft upon request.

- **Ensure freedom of association and right to collective bargaining.** Suppliers must respect workers' rights to freedom of association, collective bargaining, and peaceful assembly (including the right to refrain from such activities) in accordance with local legal requirements and responsibilities, international standards such as International

Labour Organization standards or Microsoft requirements, whichever are stricter. Workers should not be intimidated, harassed or face reprisal for exercising this right. When local laws or circumstances restrict this right, Suppliers should pursue other ways of engaging in meaningful dialogue with their workers on employment issues and workplace concerns.

- **Provide effective grievance procedures.** Suppliers must provide employees with effective grievance procedures for raising workplace concerns, including concerns involving harassment and discrimination, to the attention of management for appropriate resolution. Workers must be given a safe environment to provide their grievances and feedback. Suppliers must review these reporting procedures periodically. The grievance procedures provided must be accessible, culturally appropriate, and include the option to report anonymously where appropriate. Workers and/or their representatives must be able to openly communicate and share ideas and concerns with management regarding working conditions and management practices without fear of discrimination, reprisal, intimidation, or harassment. Suppliers must periodically provide workers with information and training on all grievance procedures. All forms of retaliation against workers for raising a workplace concern are strictly prohibited. Suppliers shall not retaliate through use of personal attacks, intimidation, or other threats against workers who act to raise workplace concerns, including infringement of worker rights under local legal requirements or international standards.

- **For Suppliers with employees physically located in the U.S. who are performing work as part of any contract with Microsoft that requires access to Microsoft facilities or network:**
    a. Supplier must make available an employee career development program.
    b. Any person staffed on a Microsoft project by Supplier must be an employee of Supplier or employee of an approved subcontractor of Supplier.
    c. Supplier must ensure that U.S.-based employees who work 30 or more hours per week for the Supplier (or for any subcontractor of the Supplier) are provided with employee health benefits that comply with the Patient Protection and Affordable Care Act of 2010 (the "ACA") and its related statutes and regulations, as amended from time to time. Such health coverage must be "affordable" and "minimum value" as those terms are defined in the ACA, and Supplier must provide this coverage to any employee staffed on a Microsoft project even if Supplier is not otherwise required to offer this coverage under the ACA. If Supplier receives notice from a government agency that this health coverage is not compliant with the ACA or that a penalty will be assessed related to this health coverage under the ACA, Supplier must provide written notice to Microsoft within 30 days.
    d. If a Supplier has more than 50 employees in the U.S., the Supplier must provide the certain minimum benefits to Eligible Supplier Employees. "Eligible Supplier Employee" is defined as any U.S.-based Employee of Supplier who has worked for Supplier for at least 1500 hours in the prior 12 months and who is staffed on a

Microsoft project or contractual agreement that requires access to Microsoft's network and/or facilities. Supplier must provide Eligible Supplier Employees with:

- At least 10 days of paid time off and 5 days of paid sick leave or 15 unrestricted days of paid time off, administered at Supplier's reasonable discretion.
- At least 12 weeks of paid parental leave at 66% of pay with a cap of $1,000 per week or an amount of paid parental leave sufficient to comply with Washington State's paid family leave law.

## HEALTH AND SAFETY

Microsoft Suppliers are required to develop and implement health and safety management practices in all aspects of their business. Without limitation, Suppliers must:

- Comply and implement a process to ensure that their employees comply with all applicable occupational health and safety laws and regulations, including but not limited to requirements that address occupational safety, emergency preparedness, occupational injury and illness, industrial hygiene, physically demanding work, machine safeguarding, sanitation, food, and housing.
- Provide a safe and healthy work environment for all employees, take action to minimize the causes of hazards inherent in the working environment, and implement controls to protect sensitive populations.
- Establish an occupational health and safety management system that, at a minimum, demonstrates that health and safety management is integral to the business, allows for leadership and encourages employee participation to set policy, roles, responsibilities, and accountabilities, provides for risk and hazard identification and assessment, and provides appropriate communication channels for employee access to health and safety information. This management system must include procedures to address incident recordkeeping, investigation, and correction action.
- Prohibit the use, possession, distribution, or sale of illegal drugs.

## ENVIRONMENTAL PROTECTION AND COMPLIANCE

Microsoft recognizes its social responsibility to protect the environment. We expect Suppliers to share our commitment by responding to challenges posed by climate change and working toward protecting the environment. As a part of this commitment, all Microsoft Suppliers must, without limitation:

- Comply with all applicable environmental laws and regulations, including but not limited to laws and regulations that regulate hazardous materials, air, and water emissions, and

wastes and laws, regulations, and customer requirements regarding the prohibition or restriction of specific substances in manufacturing or product design.

- Supplier agrees to conform to all Microsoft requirements regarding product and packaging labeling, material content, and recycling, and disposal as directed by Microsoft in their business contracts.
- Obtain and maintain all required environmental permits, regulatory approvals, and registrations.
- Prevent or eliminate waste of all types, including water discharges and energy losses, by implementing appropriate conservation measures in Supplier facilities through (1) the use of conservation-minded maintenance and production processes, and (2) by implementing strategies to reduce, reuse, and recycle materials (in that order), whenever possible, prior to disposal.
- Identify any chemicals, waste, or other materials that may be released, and which may pose a threat to the environment, and manage such chemicals or materials appropriately to ensure their safe handling, movement, storage, use, reuse, recycling, and disposal. Ozone-depleting substances are to be effectively managed in accordance with the Montreal Protocol and applicable regulations.
- Suppliers must disclose complete, consistent, and accurate scope 1, 2 and 3 greenhouse gas (GHG) emissions data and/or components required to calculate GHG emissions data, via CDP or an alternative method that Microsoft will provide. If requested by Microsoft, Suppliers must provide plans to reduce greenhouse gas (GHG) emissions in alignment with Microsoft's requirements. The timing of Supplier conformance to this requirement may be determined by Microsoft standards and requirements that are set forth in their contract with Microsoft.

## PROTECTING INFORMATION

Microsoft Suppliers must respect intellectual property rights, protect confidential information, comply with privacy rules and regulations, and adhere to Microsoft's Document Retention Policy and Retention Schedule, as applicable. All Microsoft Suppliers must, without limitation:

### Business Continuity

- Ensure maintenance of a measurable documented emergency response and disaster recovery plan to guarantee the protection of data and intellectual property and the business continuity of the services and/or goods being provided to Microsoft. The plan must include implementation procedures and at a minimum continuity and recovery plans for: weather or other natural disaster, labor or other resource constraints, system and/or facilities outage or unavailability, power outage, and telecommunication outage. The Supplier will review and test their business continuity plan at least annually to ensure it is fully compliant with industry best standards for continuity management and, without limiting the foregoing, compliant with all of Microsoft's requirements.

### Physical and Intellectual Property

- Protect and responsibly use the physical and intellectual assets of Microsoft, including intellectual property, tangible property, supplies, consumables, and equipment, when authorized by Microsoft to use such assets.
- Respect and protect the intellectual property rights of all parties by only using information technology and software that has been legitimately acquired and licensed. Use software, hardware, and content only in accordance with their associated licenses or terms of use.
- Use Microsoft-provided information technology and systems (including email) only for authorized Microsoft business-related purposes. Microsoft strictly prohibits Suppliers from using Microsoft-provided technology and systems to (1) create, access, store, print, solicit, or send any material that is intimidating, harassing, threatening, abusive, sexually explicit, or otherwise offensive or inappropriate, or (2) send any false, derogatory, or malicious communications. Any solicitation of Microsoft employees using information gathered from Microsoft-provided technology or systems is prohibited.
- Comply with the intellectual property ownership rights of Microsoft and others, including but not limited to copyrights, patents, trademarks, and trade secrets. Manage the transfer of technology and know-how in a manner that protects intellectual property rights.
- Consider all data stored or transmitted on Microsoft-owned or leased equipment as property of Microsoft. Microsoft may monitor all use of the corporate network and all systems (including email) and may access all data stored or transmitted using the Microsoft network.
- To ensure adherence to Microsoft Device Health Restrictions, if assigned an alias@microsoft.com account for your role, you will be required to access Microsoft resources only from a Microsoft managed device or you will need to use the virtualization service (Windows Virtual Desktop) in order to access resources including email, Teams or other applications or services.

**Security**

- Disclose and ensure any identified vulnerabilities are addressed immediately.
- Do not provide access to Microsoft information, or customer information, without a legitimate business need, and permission from the responsible owner.
- Do not bypass security controls, restrictions, or any other security measures.
- Do not share account credentials with others and always authenticate with assigned account credentials.
- Do not repurpose or synchronize Microsoft credentials with accounts on third-party sites.
- Maintain direct control of corporate and personal devices and lock or secure devices at all times when not in use.
- If a Microsoft asset or personal device containing Microsoft business-related data is lost or stolen, report it as soon as possible.
- Clearly display an employee access card at all times when in a Microsoft facility. Ensure visitors are registered at the reception desk with a Microsoft host. Challenge anyone not

displaying an access card and escort them to the nearest Microsoft receptionist/security point of contact.
- Keep computer software up to date and fully patched.
- Do not download or install untrusted, unlicensed, prohibited, or illegal software on any device or system that accesses Microsoft business data or services.
- Ensure personal devices that are used to conduct Microsoft business are up to date and are enrolled in the Modern Access device management system.
- Report any potential incident that involves Microsoft customer data (whether internally or through a partner or Supplier) as soon as possible.

**Privacy**

- Follow all local privacy and data protection laws.
- Provide clear and accurate privacy notices when collecting or processing personal data.
- Honor privacy choices by using data only as agreed to by Microsoft representatives or Microsoft's customers.
- Protect data by building secure products and services.
- Cooperate with Microsoft Compliance efforts.

**Retention of Corporate Records and Internal Business Information (all formats)**: The requirements below apply to all formats of information assets, globally and enterprise wide.

- All business records created, manage, or used on Microsoft premises or with Microsoft equipment/tools will be retained in full compliance with the Microsoft Document Retention Policy, Corporate Retention Schedule, and other Microsoft-directed practices.
- Unless otherwise specified, Microsoft will retain all rights of ownership, and control of all information created, managed, or used outside of Microsoft's premises and/or Microsoft equipment/tools as described in the contract with Microsoft.
- In specific instances Supplier may be required to retain, pull, or otherwise provide data to Microsoft for a prescribed amount of time as established in the contract or in the case of a legal or audit matter a hold may require data be retained beyond that obligation.

## SUPPLIER CODE OF CONDUCT TRAINING

**Training compliance**: Suppliers must ensure their employees and approved subcontractors working on Microsoft matters understand and comply with the contents of the Supplier Code of Conduct, the applicable laws and regulations and generally recognized standards.

- Supplier shall administer SCoC training on an annual basis to all employees and approved subcontractors working on Microsoft matters.
- Supplier must administer this training through the Microsoft-provided third-party training platform. For more information, review the SCoC Training Frequently Asked Questions (FAQs) on the Supplier Code of Conduct website.

- Training records and attestations of the requirements through the third-party training platform are subject to audit.

In addition to Supplier's training obligations noted above, Microsoft provides training to all External Staff requiring access credentials to the Microsoft corporate network and/or buildings before they obtain their access rights.

# ADDITIONAL STANDARDS FOR MICROSOFT ACCESS

Any External Parties, including but not limited to Suppliers, Contractors, Sub-Contractors, Consultants, Landlords, Business Guests, and Partners requiring access to Microsoft's network and/or facilities, the following additional standards apply.

## PRE-PLACEMENT/ACCESS POLICY

Suppliers, Contractors, Sub-Contractors, Consultants, Landlords, Business Guests, and Partners must conduct Pre-Placement/Access background screens that meet Microsoft requirements on all their personnel that (1) require any access to Microsoft's network, including email, SharePoint sites, or any other tool, site, platform, or (2) require unescorted access to Microsoft facilities (whether owned or leased) including being issued a cardkey, or other access badges. The purpose of such screens is to ensure that those with access to Microsoft's facilities, equipment, networks, or systems do not present undue safety or security risks.
Prior to placement of external personnel and/or provisioning the person with access, to the extent allowable by applicable law, the Supplier must register with Microsoft's Global External Staff Screening Program and conduct a Pre-placement/Access background screen under that program configured with Microsoft's designated screening service provider.

For certain personnel placements, the Supplier must conduct additional periodic background screens. To the extent allowable by applicable law, Microsoft will identify minimum background screening components, specific to each country, which must be conducted. Background screens will typically include review of the following components: identity check, criminal record review, national criminal database search, sex offender registry check, and global sanctions review. Microsoft may require additional screens, such as education verification, prior employment verification, verification of job-related licenses, consumer credit report review, drug testing, and/or other relevant information gathering if required for a specific placement.

After receiving each background screening report, Supplier must evaluate whether the Supplier's personnel are suitable to access Microsoft facilities and/or network required for their work connected to Microsoft. Specifically, Supplier must adjudicate whether the background screening report contains information such as criminal convictions or other matters that may deem the individual unsuited to perform work and/or have Microsoft provisioned access. Examples of convictions that may be reasonably related and should be reviewed by the Supplier include, but are not limited to, crimes of dishonesty (such as property or identity theft, embezzlement, fraud, forgery, etc.) and violence (such as murder, rape, sexual abuse, kidnapping, assault, robbery, stalking, harassment, etc.). Suppliers may be required to certify that they have conducted and reviewed Pre-Placement/Access screens for their personnel, consistent

with this policy. Supplier must adjudicate any criminal convictions, serious delinquency or debt, or any other matters disclosed in the background screen that may deem the individual unsuitable for Placement/Access at Microsoft.

Microsoft reserves the right to review and discuss information collected during the screening process with Suppliers for any individual requiring placement or access, including any situation that would require Supplier personnel to access credit card, financial, or sensitive personal data of Microsoft customers, partners, employees, or other third parties. Any such discussions shall be conducted consistent with applicable law. Based on that review, Microsoft may prohibit placement and/or access, as it deems appropriate, to any individual.

If a Supplier uses any sub-contractor to perform services that (1) require any access to Microsoft's network, including email, SharePoint sites, or any other tool, site, platform, or (2) require unescorted access to Microsoft facilities (whether owned or leased) including being issued cardkey, or other access badges, the Supplier must ensure that its contracts with sub-contractors include the requirements set forth in this policy. In addition, if a sub-contractor's personnel will require access to credit card, financial, or sensitive personal data of Microsoft customers, partners, employees, or third parties, the Supplier must also take reasonable steps, in compliance with applicable law, to ensure that sub-contractors conduct the required background screening, as defined in this policy.

If a Supplier becomes aware of criminal activity by their personnel or the sub-contract(s) who currently have access to Microsoft owned or leased facilities or access to Microsoft's networks, the Supplier must refer the information to Microsoft Global Security within 24 hours of becoming aware of the information to determine whether it is acceptable for such individual to continue to have access. If it is not acceptable, Microsoft Global Security will work with Microsoft Sponsor and the Supplier to remove the individual from the Microsoft assignment and ensure all access is expeditiously revoked. Suppliers must comply with all applicable laws when removing any Supplier personnel or sub-contractor(s) from Microsoft's owned or leased property. If this criminal activity suggests a possible threat of physical harm directed at Microsoft property or employees, the Supplier must immediately inform its Microsoft business contact and Microsoft Global Security, but in no event later than 24 hours after becoming aware of the information.

In all instances, Suppliers must comply with the Fair Credit Reporting Act and any other applicable federal, state, and local laws, including data privacy laws. Suppliers are responsible for providing the relevant notices and, if required, obtaining lawful consents, or establishing other lawful bases to (1) conduct the Pre-Placement/Access background screens, and (2) if required, provide Microsoft with the necessary consent required for Microsoft to receive and use that information lawfully. If requested by Microsoft, Suppliers must provide their personnel with a privacy notice or consent document, in a form approved by Microsoft, prior to conducting the Pre-Placement/Access background screens.

In addition to any indemnification obligations in the relevant contract, if any, pursuant to which Supplier was engaged by Microsoft, Supplier agrees to indemnify and hold harmless Microsoft, its affiliates and subsidiaries and their respective officers, directors, employees, agents and

insurers ("Microsoft Parties") from any and all damages, penalties, fines, losses, liability, judgments, settlements, award costs and expenses (including reasonable attorneys' fees and expenses) arising out of or in connection with any claims, assertions, demands, causes of action, suits, proceedings, investigations, enforcement or other actions, whether at law or equity ("Claims") related to (1) any breach by Supplier of this Pre-Placement/Access Policy; (2) Supplier's violation of applicable laws or ordinances related in any manner to the subject matter discussed in this Pre-Placement/Access Policy, (3) Supplier's negligence, misconduct, recklessness, errors or omissions, and/or (4) Supplier's employment decisions. Supplier shall also indemnify and hold harmless the Microsoft Parties from any Claims brought by an employee or contractor of Supplier against one or more of the Microsoft Parties related to the background screens described in this Pre-Placement/Access Policy. For clarity, the additional indemnity obligations in the Pre-Placement/Access Policy Section of the Supplier Code of Conduct apply solely in connection with Supplier's personnel access to Microsoft's facilities, equipment, networks, or systems.

For more information, review the Background Screening Frequently Asked Questions. Suppliers may direct any questions or concerns about this program to supscrn@microsoft.com.

### USE OF MICROSOFT FACILITIES AND NETWORK

- Suppliers must not use any Microsoft-provided facilities (e.g., buildings and site services) other than in performance of services provided to Microsoft without the prior written consent of Microsoft.
- When Supplier personnel require cardkey access to Microsoft facilities, an account on Microsoft's email system, and/or any other access to any of Microsoft's networks or systems, the Supplier and its personnel assigned to Microsoft must sign all applicable contract(s) required by Microsoft.
- Suppliers and their employees must not use their location on Microsoft's premises or network access to obtain information or materials or physical access other than as expressly authorized by Microsoft. Microsoft will not be responsible for loss, damage, theft, or disappearance of any personal property or vehicles located on Microsoft premises belonging to any Supplier or its employees or approved subcontractors.
- If a Supplier becomes aware that a "significant" injury to someone or damage to property has occurred on Microsoft premises, the Supplier must notify Microsoft promptly and provide adequate details to enable Microsoft to investigate the cause. "Significant" in this case means injury to a person that results in hospital treatment or death, or damage to or loss of property with an estimated repair or replacement value in excess of $10,000 USD.

## RAISING CONCERNS AND REPORTING QUESTIONABLE BEHAVIOR

- To report questionable behavior or a possible violation of the SCoC, Suppliers are encouraged to work with their primary Microsoft contact in resolving their concern. If

that is not possible or appropriate, please contact Microsoft through any of the methods described at: http://www.microsoftintegrity.com/

Microsoft will maintain confidentiality to the extent possible and will not tolerate any retribution or retaliation taken against any individual who has, in good faith, sought out advice or reported questionable behavior or a possible violation of the SCoC.