Bringing humanity to business

RISK MANAGEMENT POLICY

Purpose

Our complex global business spans multiple business segments, client industries, and geographic regions. At all relevant times, somewhere around the globe, someone at TTEC makes decisions on behalf of the company that create important obligations and potential risks for the business. The purpose of this Policy is to outline the framework of how TTEC manages risk and who at TTEC has primary and supporting responsibilities for managing various risks critical to the business.

This Policy is *a living* document, and it will continue to evolve with the needs of our business. It will be reviewed periodically and revised as necessary. Glossary of terms used in this Policy may be found in Exhibit A.

Policy Statement

It is the Policy of TTEC that we manage our risks proactively. To manage risk, TTEC (1) continuously assesses its business risks in light of relevant developments across multiple dimensions, including, but not limited to, strategic competitive risks in our business, operational risks, financial risks, technology resilience and cybersecurity risks, labor risks, legal, regulatory, and compliance risks, geopolitical and social impact risks, and climate risks; (2) periodically tests the risk tolerance[1] of our business and evaluates that tolerance against the risk appetite[2] of our Management Team and our Board of Directors; (3) communicates material risks relevant to TTEC and our risk tolerance levels to keep all relevant stakeholders informed about risks that may impact the business aspects that they control and influence; (4) requires that its business leaders manage risk relevant to their areas of responsibility proactively in alignment with TTEC risk appetite and risk tolerance; and (5) maintains a risk assurance function that provides oversight and validation for risk assessment and management activities in accordance with the Policy.

Risks We Manage

TTEC is a complex, publicly listed business with a global footprint that serves diverse commercial and public sector clients in banking, financial services, insurance, healthcare, transportation, logistics, travel, hospitality, communication, entertainment, technology, retail/e-

[1] **Risk Tolerance**: Enterprise Risk Tolerance is a financial term that speaks to the level of downside risk a company can absorb before its business and its shareholder value is materially impacted.

[2] **Risk Appetite**: Enterprise Risk Appetite is the level of risk that an organization is prepared to accept in pursuit of its objectives, and before action is deemed necessary to reduce the risk. It represents a balance between the potential benefits of risk taking and innovation and the threats that change inevitably brings.

tail, citizen services, and other business verticals with next-gen digital technology, AI-enabled digital CX solutions and analytics to support omnichannel contact centers, CRM, customer engagement, acquisition and growth, tech support, back office functions, and fraud prevention.

The risks that TTEC prioritizes to support this broad business remit vary from time to time, but usually include the following in no particular order:

- ✓ Strategy Execution
- ✓ Robustness of Financial Structures and Liquidity
- ✓ Service Delivery Excellence
- ✓ Labor related risks
- ✓ Responsible AI Enablement
- ✓ Technology Resilience
- ✓ Cybersecurity Effectiveness
- ✓ Global Data Privacy and Data Governance
- ✓ Information Security and Data Privacy risks
- ✓ Global Regulatory Obligations
- ✓ Global Compliance Effectiveness
- ✓ Risks Inherent in our Geographic Footprint
- ✓ Health & Safety
- ✓ Fraud
- ✓ Social Responsibility and related Reputational risks

Risk Culture

The Company is committed to fostering a strong and transparent risk culture that promotes accountability, open communication, and sound decision-making across all levels of the organization.

TTEC Risk culture is set by the Board of Directors and executive leadership team under the leadership of TTEC the Chief Executive Officer (CEO). The Leadership Team is responsible for modeling appropriate risk behaviors, reinforcing the importance of integrity and accountability, and ensuring that risk management principles are consistently applied throughout the organization. This commitment is reinforced through regular communication, training, and performance expectations.

Together, these elements support a culture where risk awareness is embedded in daily activities, and where all employees contribute to the effective management of risks in pursuit of the Company's strategic objectives.

Employees at all levels in the organization are expected to proactively identify, assess, and escalate risks within their areas of responsibility. Business segment leaders and functional management are responsible for identifying, assessing, proactively managing, and monitoring risks within their areas of responsibility. This includes implementing effective controls, operating within approved risk appetite and tolerance levels, and ensuring timely escalation of risks in accordance with Company policy.

Risk Management, Compliance, Legal, and other oversight functions provide independent guidance, monitoring, and challenge to the business segment and functional management teams. These functions are responsible for establishing risk frameworks, policies, and methodologies; facilitating enterprise risk assessments; monitoring adherence to risk appetite; and supporting regulatory compliance. Risk Management, Compliance, and Legal also coordinates risk reporting and escalation to executive leadership and the Board. Internal Audit

serves as the independent assurance function, providing objective evaluation of the effectiveness of risk management, internal controls, and governance processes. Internal Audit operates independently of management and maintains a functional reporting relationship to the Audit Committee of the Board of Directors to preserve its objectivity and authority.

The Company maintains a strict non-retaliation policy, and individuals who raise concerns or report potential risks in good faith will be protected from any form of adverse treatment. Timely and transparent escalation of risks is essential to effective risk management and organizational resilience.

Risk-informed decision-making is a core expectation and is embedded into the Company's business processes, strategy development, and operational activities. Employees are encouraged to consider both the potential risks and opportunities associated with their decisions, and to seek guidance where appropriate to ensure alignment with the Company's risk appetite and tolerance.

Periodically, the Risk Management framework, processes, and practices are reviewed for program effectiveness and identification of opportunities to continuously improve the program. Effectiveness of the program includes adequate support of the identification, assessment, and management of material risks. Improvement initiatives may be informed by lessons learned from risk events, audit findings, changes in operating environment, evolving standards and industry best practices, and stakeholder feedback.

Escalation & Reporting

The Company maintains a formal risk escalation framework to ensure timely identification, evaluation, and communication of material risks in accordance with regulatory requirements.

Employees with risk ownership or oversight responsibilities, including managers, business unit leaders, and responsible personnel within control functions, are expected to proactively identify and escalate risks within their areas of responsibility in accordance with the escalation channels outlined in the relevant company policies and/or standard operating procedures. Risks must be escalated when they could reasonably be expected to have a material impact on the Company's business, operations, financial condition, results of operations, strategy or reputation. This includes, but is not limited to, material cybersecurity exposure, regulatory compliance gaps, adverse financial developments, health and safety concerns, legal contingencies, and operational disruptions.

Failure to timely escalate a suspected or known material risk in accordance with the protocols established by the relevant policies will be addressed through the Company's performance management process and may result in disciplinary actions including termination.

Potential material events must be reported immediately (generally within 24 hours) to relevant functional leaders (e.g., Risk Management, Legal, Compliance, Information Security, Finance, etc.). A cross-functional team will assess materiality without unreasonable delay, consistent with best practices.

Material risks are escalated from operational management to executive leadership, including the CEO, and, where appropriate, to the Audit Committee outside of the regular reporting cycle. The Company maintains disclosure controls and procedures to support timely escalation, documentation, and compliance with reporting obligations.

This framework is complemented by ongoing risk reporting, including quarterly updates to the Audit Committee and periodic reporting from key risk leaders, and is integrated into the Company's enterprise risk management processes.

How We Identify and Test Our Risks

The Company recognizes the importance of proactively identifying, assessing, and managing emerging risks that may impact on its long-term strategic objectives. Emerging risks are monitored as part of the Company's Enterprise Risk Management processes and are subject to appropriate governance, oversight, and escalation. These insights are to assist during business decisions for business resource / capital allocation, performance management, risk-transfer decisions, new country/market entry, acquisitions, strategic planning and partnerships, or other material transactions. Management shall consider both expected strategic benefits and risk-adjusted returns, including the likelihood, severity, mitigation cost, transferability, and residual risk associated with the proposed action. Material risk considerations shall be documented and escalated to the Executive Leadership Team (ELT) and, where appropriate, to the Board or applicable Board committee.

To identify and proactively manage its risks, TTEC performs several distinct and separate risk discovery exercises that vary from time to time, but at a minimum include:

(1) Periodic Enterprise Risk Management (ERM) assessments / exercises;
(2) Annual holistic risk factors identification process;
(3) Technology resilience testing;
(4) Cybersecurity vulnerability assessment and testing;
(5) Legal & regulatory review;
(6) Annual Internal Audit program; and
(7) Annual external independent audit review.

The Enterprise Risk Management Exercise

Enterprise Risk Management exercises are conducted periodically by the TTEC Risk Department in partnership with Finance, Operations, IT and Human Resources organizations. The cadence of this review is based on evolving developments in the TTEC risk environment, the industries it serves, and its clients. A comprehensive ERM assessment is generally conducted every year, or more frequently as warranted by material changes in the Company's risk profile. Additionally, emerging risks that are identified may warrant an ad hoc assessment regardless of scheduled exercise cycle to understand potential business impact and mitigation processes. In the years when a formal ERM assessment is not conducted, the prior years' risk assessment findings are nevertheless reviewed and refreshed in consultation with the TTEC Management Team and its Audit Committee of the Board of Directors.

The approach to the ERM may vary year to year but usually falls into one of the following categories (or a variation on the same): (1) a comprehensive survey of key enterprise leaders in each business segment, business vertical, business function, and key geographies; and/or (2) an interview with members of the ELT, their direct reports, and members of TTEC Board of Directors with in depth, open-ended questions; and/or (3) a comprehensive holistic review of global risks as seen by global public and private thought leaders, and by global consultancy firms and testing these risks against TTEC business environment and marketplace. In any given ERM year, the TTEC Chief Legal & Rick Officer (CLRO), in consultation with the company's

Chief Financial Officer (CFO), and the Audit Committee of the Board of Directors, may use any of these three ERM approaches or a combination of any of them.

In performing the ERM exercise, the TTEC leaders are asked to consider key risks across three different dimensions:

(1) Likelihood of Occurrence (remote to highly probable)
(2) Impact on TTEC in terms of Severity (low to high – minimal impact to catastrophic impact)
(3) How well TTEC is positioned to manage the risk (well to not at all)

The findings are analyzed with top risks based on likelihood of occurrence, severity of impact, and TTEC preparedness and are then summarized and presented for subsequent review to TTEC ELT and TTEC Audit Committee of the Board.

Once top risks are identified and agreed, each risk is assigned to the risk owner and a project manager, who develop comprehensive risk management and mitigation plans. Risk owners, generally members of the TTEC ELT, in coordination with Risk Management and relevant oversight functions, shall monitor performance and report material trends and updates during the course of the year in which CLRO delivers a quarterly update to the Audit Committee of the Board. See Exhibit B, for ERM Lifecycle schematic.

In addition to Enterprise Risk Management exercises, the TTEC Risk Department conducts periodic risk appetite and risk tolerance exercises that describe the categories and levels of risk the company is willing to accept in pursuit of its strategic objectives and include measurable tolerance levels, as appropriate.

The approach to risk appetite is generally completed via a comprehensive questionnaire. Risk appetite statements are categorized into the following areas: Strategy, Financial, Operational, Reputational, Technology/Cyber/AI, Legal & Insurance, and P&C. The responses are analyzed, providing the appetite by business function and the enterprise holistically. Risk tolerance threshold is conducted via a review of standard financial metrics utilized by the company and the industry to understand the amount of loss TTEC can absorb in the aggregate in any one year without materially impacting the business. Once the range has been estimated, the CLRO interviews the CFO in consultation with the ELT and relevant risk owners to verify and agree range is correct based on current company conditions. Risk appetite and tolerance threshold levels are reported to the Audit Committee of the Board of Directors for review and feedback. Once agreed upon, these risk metrics are communicated and cascaded to business segment and function leaders to be used operation decision making, risk mitigation planning, risk transfer decisions, and escalation determinations.

Risk Factors

Annually in January of each year, CLRO identifies, with extensive input from the TTEC ELT, various risk factors that can reasonably be expected to impact the company's business and its results of operation. The list of these risk factors is organized in order of their significance to the business and the likelihood and severity of their potential impact on TTEC's results of operations, and disclosed as Part I, Item A of TTEC Annual Report to Shareholders on Form 10K.

While there can be, and usually is, a certain overlap among the risks identified and prioritized for mitigation, as part of the ERM program, and the risk disclosed as the Risk Factors in the Annual Report on Form 10K, the ERM risks are the risks that the business is currently experiencing and which must be addressed or transferred to preserve the business, the risks disclosed as part of

the Risk Factors in TTEC's annual public filings enumerate most risks that could reasonably impact the business, not just risks that the business is currently experiencing.

Technology Resiliency Testing

The company continuously assesses the effectiveness, reliability and resilience of its technology solutions (both the 'back office' technology and the client facing technology), and maintains the on-going improvement programs to keep its technology solutions current. The Chief Information Officer (CIO) and their team periodically assess the risks inherent in TTEC technology solutions and plans, implement and test on-going risk mitigation plans. As part of TTEC risk management program, the Company's IT controls are tested from time to time in connection with the annual SOX controls testing program.

The company implemented and actively maintains comprehensive business continuity, disaster recovery, and incident response plans to guide its actions during incidents, disasters, and other events requiring resilient technology operations. To strengthen preparedness for potential disruptions to critical business functions and essential technologies, we regularly conduct both live and tabletop crisis management exercises. Each exercise is followed by structured after-action reviews and documentation, including the assignment of responsible owners and resolution timelines. These follow-ups are designed to address identified gaps and continuously improve the overall technology resilience program.

Periodically, at least once quarterly, TTEC CIO reports to the ELT on evolving technology resilience risks and how the Company is addressing and mitigating these risks.

Cybersecurity Assessment and Testing

The company engages in periodic cybersecurity resilience risk assessments based on methodology and guidance from a recognized national standards organization, and utilizes periodic risk-based analysis for adopting, maintaining, and adjusting security controls to address such risks.

The following factors, among others, are considered by the Company in assessing its cybersecurity risks, mitigation, and remediation strategies: the likelihood and severity of risk; impact on the Company and on others, if a risk materializes; feasibility and cost of controls; and impact of controls on operations and on others. The specific controls used by the Company vary based on the specific systems, but usually include firewalls, intrusion prevention and detection systems, anti-malware technical safeguards and access controls, endpoint threat detection and response (EDR), identity and access management (IAM), privileged access management (PAM), logging and monitoring using security information and event management (SIEM), multi-factor authentication (MFA), vulnerability and patch management, third-party dark web monitoring and threat intelligence services.

The Company periodically tests its cybersecurity policies, standards, processes, and practices. The testing conducted by our in-house security teams includes audits, assessments, tabletop exercises, threat modeling, penetration testing, and other exercises focused on evaluating the effectiveness of our cybersecurity measures and planning.

The Company also regularly engages third parties to perform assessments on our cybersecurity measures, including information security maturity assessments, audits, and independent

reviews of our information security control environment and operating effectiveness. Individual controls are evaluated and periodically improved through vulnerability assessments and cybersecurity threat intelligence. The Company adjusts its cybersecurity policies, standards, processes, and practices as necessary based on the information provided by these assessments, audits, and reviews.

Periodically, at least once quarterly, TTEC Chief Information Security Officer (CISO) reports to the ELT on evolving cybersecurity risks and how the Company is addressing and mitigating these risks.

Data Governance and Privacy

The company maintains an enterprise-wide framework for data governance and privacy to ensure that data is managed as a critical business asset while protecting the rights of individuals and meeting legal and regulatory obligations. This framework is designed to identify, assess, mitigate and monitor risks associated with the collection, use, storage, sharing, and disposal of data.

This section establishes the risk management expectations for data governance and privacy and is supported by the company's global privacy policy and data governance policy which serve as the authoritative sources for detailed requirements and procedures.

TTEC assigns clear accountability for data management, protection, and oversight across the enterprise. Senior leadership maintains the ultimate responsibility for governance, security posture, and regulatory compliance. Data owners and data stewards are accountable for the integrity, quality, and appropriate use of data within their domains. The Chief Privacy Officer (CPO) oversees privacy compliance, regulatory alignment, and adherence to privacy principles globally. Security and technology leaders (e.g. CIO & CSO) are responsible for ensuring the appropriate safeguards for data protection and system integrity.

The company applies a risk-based approach to data classification and handling to protect information based on its sensitivity and regulatory requirements. Data is classified and managed according to defined standards to ensure appropriate levels of protection. Access to data is restricted to authorized individuals based on the business need and least privilege principles. Use, sharing, and transfer of data, including 3rd party sharing, must be controlled, justified, and compliant with applicable laws and contractual obligations.

TTEC embeds privacy-by-design principles into its data governance framework. Personal data is processed lawfully, fairly, and transparently, and limited to defined and legitimate purposes. Data minimization is applied to ensure only necessary data is collected and retained. Individuals are provided with rights such as access, correction, deletion, objection, in accordance with applicable laws and regulations.

Data is managed throughout its lifecycle to ensure quality, integrity, and compliance. Data must be accurate, complete, and reliable for its intended use. Data is retained only as long as necessary to meet business, legal, and contractual requirements and is securely disposed thereafter. Data transfers, including cross-border transfers, must comply with legal safeguards and contractual requirements.

Company implements controls to protect data from unauthorized access, loss, or misuse. Sensitive data is protected through technical and organizational safeguards such as encryption and access controls. 3rd parties must demonstrate adequate data protection controls and are contractually bound to meet privacy and security obligations.

TTEC maintains processes to identify, report, and respond to data-related risks and incidents. Employees must promptly report suspected data breaches or security incidents through established channels. Data governance roles are responsible for escalating issues impacting data quality, integrity, or compliance. In risk events related to data are incorporated into the TTEC Enterprise Risk Management processes for monitoring and remediation. Ongoing monitoring, audits, and reviews are conducted to assess adherence to data governance and privacy requirements. Training is provided to personnel with access to sensitive data to ensure awareness of obligations. Policy compliance is enforced, and violations may result in disciplinary action, including legal consequences.

Finally, the business complies with all applicable data protection and privacy laws across all jurisdictions in which it operates. Data processing activities must align with global regulatory requirements such as GDPR, CCPA, HIPAA and other applicable laws.

AI Governance

The Company maintains governance processes for the responsible development, procurement, deployment, and use of artificial intelligence and AI-enabled technologies. These processes shall address model risk, data quality, privacy, cybersecurity, bias, fairness, transparency, explainability, human oversight, intellectual property, contractual commitments, and compliance with applicable laws and regulations in jurisdictions where the Company operates. AI-related risks shall be assessed before deployment, monitored throughout the lifecycle of the relevant use case, and escalated where the use of AI may create material legal, regulatory, client, operational, reputational, or ethical risk.

Legal and Regulatory Review

The Legal and Regulatory Review is performed throughout the year by the TTEC Legal Department. At the beginning of the year (Q1), TTEC Chief Legal Officer, or designees, reviews the prior year's Legal and Regulatory developments and priorities, focusing on material laws and regulations that apply to TTEC's business. As a complex business spanning 20+ countries and six continents around the globe, TTEC is focused on material laws and regulations only, the compliance (or lack of compliance) with which may adversely impact TTEC, its business, its client service delivery or its clients. This analysis is enabled through consultation with subject-matter experts in jurisdictions where TTEC does business and delivers services, ongoing monitoring of proposed, enacted, and published laws and regulations in key jurisdictions, and the use of AI-enabled tools for ongoing alerts of developments in key areas of regulatory compliance and laws.

As the comprehensive list of laws and regulations relevant to our business is updated throughout the year, members of the Legal Department consider its impact on the business, assess potential risks of compliance and provide timely briefings to affected stakeholders in business segments and functions; they also work with TTEC program management office (the PMO) to plan and implement compliance initiatives to reduce and proactively mitigate risks presented by new or evolving laws and regulations.

Finally, at the end of the year (during Q4), the Legal Department does a comprehensive sweep of any new laws adopted by relevant legislation that may come into effect as of the 1st of the following year and provides an update to business stakeholders whose functions may be impacted by the changes.

Periodically, at least quarterly, the TTEC CLRO updates the Board on the emerging legal and regulatory risks that may have a material impact on the business. Further, at least annually, the TTEC CLRO and Chief Privacy & Compliance Officer provide a briefing to the Audit Committee of the TTEC Board of Directors and the Security & Technology Committee of the Board on evolving legal and regulatory risks that may impact financial operations of the business and/or the business compliance with public company financial reporting requirements, technology resilience and cybersecurity regulations risks and the steps being taken to mitigate such risks.

Internal Audit Program

The internal audit function at TTEC is managed by the Chief Audit Executive ("CAE") appointed from time to time by the Audit Committee of the Board of Directors, in consultation with the TTEC CFO and CLRO. In fulfilling the duties of the Chief Audit Executive, the CAE maintains full independence, has unrestricted access to the Board of Directors, and reports directly to the Audit Committee. The CAE maintains a functional reporting relationship to the Audit Committee and may maintain an administrative reporting relationship to management, provided such relationship does not impair Internal Audit's independence or objectivity. Internal Audit performs its responsibilities in accordance with applicable professional standards.

TTEC's Internal Audit function conducts an annual assessment of business risks by interviewing key executives across business segments, functions, and geographies to identify key concerns and risks. The assessment provides input for the development of a risk-based Internal Audit Plan that is presented to the Audit Committee of the Board for input and final approval. The Internal Audit Plan is designed to provide independent assurance regarding the design and operating effectiveness of governance, risk management, and internal control processes established by Management to address key business risks.

As the Internal Audit function tests the controls in the business, it identifies opportunities for improvement and communicates observations, control deficiencies, governance gaps, and process improvement opportunities to management. Management is responsible for developing and implementing corrective actions to address identified issues. The CAE presents the findings of the internal audits and the status of management remediation activities and significant risk matters to the Audit Committee quarterly.

External Audit

As a public company, TTEC is subject to an annual independent audit by a public accounting firm. As part of these audit services performed on behalf of the Audit Committee of The Board, TTEC's independent public auditors provide the Board of Directors and TTEC Management with their view on key risks impacting the business. These reports occur at least annually and usually more often.

How We Promote Risk Awareness, Training and Communication

It is the Policy of TTEC that its Management must be informed about risks relevant to the business. To that end, CLRO and CFO (through their designees) consult with various process owners and provide (or cause them to provide) periodic reports to the Management Team about existing or evolving risks and steps that the business must take to mitigate them. The process owners also provide periodic training for risks deemed material to the business. The training is provided via the TTEC learning platform, in one-on-one sessions, through Company communications, via FAQ and other tools and communication channels, distributed to those whose functions in the business may be impacted by the risks and who are in the best position to mitigate such risks or help others to mitigate them. Employees are provided role-based training in accordance with Compliance Training Policy.

How We Manage Risk Every Day

It is the responsibility of each member of the TTEC Management Team (VP and above) to proactively manage risks that are inherent in the business segment or function that she/he is responsible for. The risk management must be performed proactively, appropriately budgeted, and rolled out based on enterprise **Risk Appetite** as determined by the CEO and the ELT, and enterprise **Risk Tolerance** as determined by the company's CLO and CFO, from time to time.

If risk cannot be managed based on the Company's appetite and tolerance, it must be transferred (with insurance or risk sharing with others). Each process owner must report the status of their risk management activities and recommend to the ELT whether the risk is within tolerable levels or whether it must be transferred.

Risk Transfer

In performing its comprehensive risk assessment, TTEC determines which risks it can manage through mitigation, which it can transfer because mitigation is not possible or too expensive, and which it cannot mitigate or transfer and must therefore absorb.

To that end, TTEC manages a comprehensive multi-layered risk transfer program and annually procures property, management liability, errors & omissions, cybersecurity, and general liability insurance programs tailored to the needs of the business. TTEC CLRO and CFO determine the level and structure of TTEC's insurance needs and procure insurance based on the cost-benefit analysis of available options, informed by TTEC's risk appetite and risk tolerance analysis. The cost of insurance is considered an ordinary cost of doing business. It is budgeted annually and is reflected in the TTEC cost structure and annual management business plan.

Risk Management Oversight and Assurance

The responsibility for design of the structure and assurance functions of TTEC Risk Management Program resides with TTEC CLRO in partnership with TTEC CFO. All risk management functions are performed collectively by TTEC Finance, Business Segment, IT, Information Security, People & Culture, Risk & Legal, Regulatory Compliance, and Internal Audit organizations.

TTEC Board of Directors has the oversight responsibility for TTEC Risk Management as follows:

- Our Board oversees and regularly reviews risks inherent in TTEC's business with emphasis on the oversight of the appropriateness of the Company's risk management strategy, long- and short-range risk mitigation planning, and the effectiveness of our risk strategy execution.
- The Audit Committee of the Board reviews our overall enterprise risk management policies and practices, is actively involved in the oversight of our ERM program, and reviews risks inherent in our internal controls over financial reporting; risks specific to our geographic footprint and its expansion and concentration; risks specific to our complex regulatory compliance framework around the world; risks arising from macro- and microeconomic volatility and the related impact on TTEC clients' and our business outlook; responsible AI utilization risks; risks specific to our cost structure; and has oversight responsibility for our financial structures and liquidity risks.
- The Compensation Committee of the Board evaluates risks associated with TTEC's management and employee compensation plans; the structure of and risks specific to our employees' and senior management incentive programs, including whether those programs create an appropriate balance between financial performance and the company's

commitment to integrity and sustainability in the business; risks specific to TTEC employment practices including the Company's commitment to equality and inclusion in the TTEC workforce; and risks inherent in hiring, retention, and development of our people.

- The Nominating and Governance Committee of the Board is focused on risks inherent in our governance, senior management, and board succession planning, onboarding, and turnover; risks specific to crisis management and crisis response; and social responsibility risks specific to our business.
- The Security and Technology Committee of the Board oversees and reviews risks inherent in TTEC's IT resilience, including stability of TTEC technology stock, TTEC's cybersecurity initiatives designed to protect TTEC's IT infrastructure and data, which include the data of the Company's clients, their customers, and TTEC employees; risks specific to our data governance, including how we collect, store, use, transfer, and protect information; the Company's incident response and business continuity and disaster recovery practices.

Applicability

This Policy applies to TTEC Holdings, Inc., and all its subsidiaries and controlled affiliates, anywhere in the world, including all acquired companies subject to earn-out provisions, or shared ownership, whether they trade under the TTEC brand or as part of a different trading platform, as long as TTEC has a direct or a beneficial controlling interest in the entity (collectively, the "Company.")

Except for the Board's delegation of authority to Management, the provisions in this Policy supersede any other policies or governing documents that may contain authorizations or directions contrary to this Policy. If you are aware of any document that conflicts with this Policy, please bring it to the attention of the Legal Department to enable the harmonization of any conflicting provisions.

Responsibility

The overarching responsibility for the TTEC Risk Management Program resides with the TTEC Chief Legal & Risk Officer (CLRO) and the TTEC Chief Financial Officer (CFO). All Risk Management functions are performed in partnership with the Company's Finance, Business Segments, IT, Information Security, People & Culture, Regulatory Compliance, and Internal Audit organizations.

The members of the TTEC Executive Leadership Team (ELT) and their direct reports are responsible for the communication, implementation, and enforcement of this Policy. A failure to comply with this Policy will subject the employee to disciplinary actions, up to and including termination.

Exceptions

There are no exceptions to the Policy, but the Policy may be amended and expanded as directed by the TTEC's Chief Executive Officer (CEO) or his designees, from time to time, or by the Audit Committee of the Board.

Related Documents

This Policy is aligned with other TTEC governance policies and procedures, including without limitation:

- **Board Delegation of Authority to Management;**
- **TTEC Signature Authority Policy;**
- **TTEC Insider Trading Policy;**
- **TTEC Policy on Policies;**
- **TTEC New Country Entry Policy;**
- **TTEC Anti-Corruption Policy;**
- **TTEC Compliance Policy including Compliance Framework Matrix;**
- **Global Privacy Policy;**
- **Crisis Management – Cyber Resiliency Escalation Workflow**
- **Disclosure Policy and Disclosure Committee Charter**
- **TTEC Hiring Guidelines.**
- **TTEC Compliance Training Policy**

If you are aware of any document that conflicts with this Policy, please bring it to the attention of the Legal Department to enable the harmonization of any conflicting provisions.

Last Revised July 28, 2026

EXHIBIT A: Glossary and Definitions

- **Enterprise Risk Management (ERM):** A structured, organization-wide approach to identifying, assessing, managing, and monitoring risks that may impact an organization's ability to achieve its objectives, with the goal of aligning risk exposure with risk appetite and enhancing decision-making and value creation.

- **Risk Tolerance**: Enterprise Risk Tolerance is a financial term that speaks to the level of downside risk a company can absorb before its business and its shareholder value is materially impacted.

- **Risk Appetite**: Enterprise Risk Appetite is the level of risk that an organization is prepared to accept in pursuit of its objectives, and before action is deemed necessary to reduce the risk. It represents a balance between the potential benefits of risk taking and innovation and the threats that change inevitably brings.

- **Risk Matrix**: A visual tool used to evaluate and prioritize risks by plotting their likelihood and impact, helping organizations identify which risks require the most attention and resources.

EXHIBIT B: ERM Life Cycle