TTEC HOLDINGS, INC.
SECURITY AND TECHNOLOGY BOARD COMMITTEE
CHARTER

There shall be a Committee of the Board of Directors (the "Board") of TTEC Holdings, Inc. (the "Corporation") to be known as the **SECURITY AND TECHNOLOGY COMMITTEE** (the "Committee") with the purpose, composition, authority, duties, and responsibilities, as follows:

A. PURPOSE OF THE COMMITTEE

The Security & Technology Committee is appointed by the Board on the recommendations of the Board's Nominating and Governance Committee to play a leadership role in the risk management oversight of the Corporation's security practices and resiliency capabilities of the technology that it uses to support its business and deliver services to its clients, including the oversight of the practices and controls that management uses to identify, manage and mitigate risks related to cybersecurity, disaster recovery, cyber event management and response, fraud and physical security.

B. GOVERNANCE – COMPOSITION, MEETINGS

The Security & Technology Committee shall consist of at least two members, each of whom is a member of Corporation's Board of Directors and has experience in cyber security, technology and/or other related fields. The members of the Security & Technology Committee and the Committee's chair are appointed annually by the Nominating and Governance Committee of the Board.

The work of the Committee may be supplemented by the experts who can join the work of the Committee at the Committee chair's request but are not the actual members of the Committee.

The Security & Technology Committee of the Board shall hold regular meetings at least [twice] annually or more often at the Committee chair's discretion, generally in conjunction with the regularly scheduled meetings of the Board of Directors, and such special meetings as the chair of the Committee or the Chair of the Board may direct from time to time.

Committee meetings may be held in person or via digital technology, and at such times and places as the chair of the Committee deems appropriate. In addition to formal meetings, the Committee may act by unanimous written consent with proper materials provided to take an informed decision.

Although it is expected that most of the Committee's work will be performed as part of regularly scheduled meetings, the Corporation's Chief Security Officer, Chief Information Officer, Global Chief Operating Officer and lead Internal Auditor (or others with different titles but carrying the responsibilities reflective of these roles) may have direct and independent interaction with the Committee chair from time to time or the full Committee, as the Committee chair deems appropriate.

The Committee may form and delegate authority to subcommittees when appropriate.

The Committee may invite members of management and outside consultants to participate in its meetings, provided however, that it shall also meet in the executive session (with only Committee members present) as appropriate. It is generally accepted that the Chief Security Officer, Chief Information Officer, Chief Operations Officer, Chief Risk Officer and the head of the Corporation's internal audit function would attend the meetings of the Committee.

Any action taken by the Security & Technology Committee pursuant to the authority conferred under this Charter shall for all purposes constitute an action duly and validly taken by the Board of Directors and may be certified as such by the Secretary or other authorized officer of the Corporation.

C. DUTIES AND RESPONSIBILITIES

The duties and responsibilities of the Committee shall include the following, and may be modified from time to time by the decisions of the Board or the Nominating & Governance Committee on delegation from the Board:

In performing its oversight responsibilities, the Committee shall:

1. Review, on an annual basis, the management's security, technology, fraud prevention, and resiliency strategic plans for the Corporation.

2. Review the management's implementation of Corporation's cybersecurity, cyber risk management, technical resiliency programs; and fraud and physical security mitigation plans, including potential external and internal threats, and threats arising from transactions with trusted third parties and vendors.

3. Review the programs that the management deploys to educate employees about relevant information security, physical security and fraud issues and Corporation's policies with respect to security and fraud.

4. Review the management's crisis preparedness and incident response plans, and the Corporation's disaster recovery plans, capabilities, and testing practices.

5. Review the management's corrective actions for deficiencies that arise with respect to the effectiveness of the cyber security and resiliency programs.

6. Review the Corporation's internal and third party security compliance audits.

7. Review, at least annually, risk assessments relevant to the Corporation's security and technology conducted by, or on behalf of, the Corporation.

8. Review projected spend and budgets related to security and fraud controls and resourcing.

9. Review the adequacy of the Corporation's insurance programs to determine if the coverages are sufficient, consistent with market conditions, to protect the Corporation.

10. Receive information from and engage in the robust dialog with the Chief Security Officer (or another senior executive with responsibilities for Corporation's security) regarding matters related to the management of cybersecurity, physical security, and fraud.

11. Receive information from and engage in the robust dialog with the Chief Information Officer (or another senior executive with responsibilities for Corporation's information technology) regarding matters related to the management of technology security and resiliency capabilities.

12. Periodically, but at least once annually, review with the Board
    (i) the Corporation's technology and security related strategies including planned investment levels for the execution of such strategies.
    (ii) the framework that the Corporation uses to prevent, detect, and respond to cyber incidents, physical and fraud incidents, physical attacks and systems or data breaches.

13. Address other matters as the Committee members determine relevant to the Committee's oversight of the Corporation's security and technology risk management practices.

D. AUTHORITY AND RESOURCES

The Committee shall have the authority to take appropriate actions necessary to discharge its responsibilities, and shall have access to resources to do so. The Committee may hire and retain, at

the Corporation's expense, cybersecurity consultants, outside counsel and other advisors to assist it in the performance of its functions.

The Committee members may seek and receive any information from management and others in the Corporation, as it deems appropriate in the fulfillment of its functions.

E. MINUTES AND REPORTS

The Committee shall keep track of its activities by keeping minutes of topics discussed and actions taken. The Committee may rely on the Corporate Secretary to produce the minutes of each meeting (except the executive sessions where the Committee shall have discretion to keep or not to keep minutes as it deems appropriate). The minutes of all meetings shall be reviewed and approved (with modifications as necessary) by the Committee members at the next regularly scheduled meeting. The Committee chair shall produce a summary of topics discussed and actions taken at each Committee meeting and present them to the Board at the next regularly scheduled Board meeting.

F. COMMITTEE CHARTER REVIEW

The Committee shall annually review and reassess the adequacy of this Charter and recommend to the Board any changes it considers necessary or advisable.

Established: May 26, 2022