Bringing humanity to business.

# TTEC Information Security Risk Management Policy

## I. PURPOSE

This policy helps TTEC Holdings, Inc. and its subsidiaries (the "Company") identify, estimate and prioritize potential risks and vulnerabilities to the confidentiality, integrity, and availability of Protected Health Information (PHI) and Personally Identifiable Information (PII) that it maintains on behalf of clients as well as take appropriate steps to mitigate any identified risks and vulnerabilities. The Information Security Risk Management Policy will help leaders make informed decisions about information security risk mitigation by identifying:

- Relevant threats to the Company.
- Internal and external vulnerabilities.
- The impact to the Company that may occur given the potential for threats exploiting vulnerabilities.
- The likelihood that harm will occur.

This policy is intended to cover the potential risks and vulnerabilities to the confidentiality, availability and integrity of all PHI and PII that the Company creates, receives, maintains or transmits on its own behalf or on behalf of its clients. This policy supports the Company's compliance efforts, including compliance with HIPAA, HITRUST, PCI-DSS, SOX, SOC 1, SOC 2, ISO 27001, FISMA and FedRAMP as updated from time to time. This policy applies to the Company's information security efforts. It does not apply to other risk management initiatives.

## II. POLICY STATEMENT

It is the policy of the Company to proactively manage risks and vulnerabilities to the confidently, availability and integrity of all PHI and PII that the Company creates, receives, maintains or transmits directly or on behalf of its clients. The Company implements an integrated control system characterized using different control types (e.g. layered, preventive, detective, corrective, and compensating) that mitigates identified risks. As part of its risk management responsibilities, it is the policy of the Company to conduct period risk assessments as provided in this policy and related SOPs. It is also the policy of the Company to develop annual risk management and treatment plans based on the risk assessments performed, developing, implementing and updating controls as reasonable and appropriate after considering relevant factors, including the following:

- The size, complexity and capabilities of the Company.

- The Company's technical infrastructure, hardware and software security capabilities.
- The costs of security measures.
- The probably and criticality of potential risks to PHI.

The Company purchases appropriate insurance to cover its business risks, including those related to remote workers and employees.

This policy will be periodically reviewed in accordance with the requirements of the Policy on Policies.

**Risk Assessment Methodology**

The Company follows the following methodology when conducting risk assessments:

- It follows the risk assessment process set forth in the Risk Assessment SOP.
- It uses the risk model set forth in the Risk Assessment SOP.
- It uses a quantitative approach, a qualitative approach or a combination of both. • It uses an impact oriented approach to analyzing risk.
- It evaluates multiple factors that may impact security as well as the likelihood and impact from a loss of confidentiality, integrity and availability of information and systems.

**Acceptable Levels of Risk**

Acceptable levels of risk have been determined by the Healthcare Compliance Committee. The decision on whether to mitigate further, and which additional controls are appropriate, should take into consideration the practicality (cost and additional burden) of, and the additional security achieved by, further mitigation.

| Risk Level | Score | Action |
|---|---|---|
| Low | 1.0 – 2.0 | No action required. |
| Moderate | Greater than 2.0 and less than 6.5 | Requires review to determine whether the risk should be further mitigated. Acceptance of the risk without mitigation requires Healthcare Compliance Committee approval. |

| | | |
|---|---|---|
| High | Equal to, or greater than, 6.5 | Requires additional mitigation. Acceptance of the risk without additional mitigation requires Executive Committee approval. |

**Continuous Risk Management**

The Company practices continuous risk management, which includes performing risk assessments as set forth below. The Company uses a risk based approach when mitigating risks to the confidentiality, integrity and availability of information. Controls should be more stringent when there is a higher likelihood that a threat will occur or when the impact will be high and less stringent for low likelihood/low impact threats. The organization updates the risk assessment before issuing a new formal authorization to operate or within every three (3) years, whichever comes first, or when conditions occur that may impact the security or authorization state of the system.

*Enterprise Information Security Risk Assessments*

The process for performing an enterprise information security risk assessment is set out in the Enterprise Information Security Risk Assessment SOP. Risk assessments will be performed and reevaluated annually or more frequently if there is a significant change to the information system or operational environment or whenever a new significant risk factor is identified. The results of the risk assessment will be shared with the IT Steering Committee to help the Company mitigate risk identified by the assessment and identify areas of risk that the Company is willing to accept.

*Information System Risk Assessments*

The Company performs risk assessments of those information systems which store, maintain, receive or transmit PHI or PII at least annually, in accordance with the Information Systems Risk Assessment SOP. Risk assessments will also be performed if there is a significant change to the information system or the operational environment or whenever a new significant risk factor is identified. Information systems risk assessments shall use a risk based approach to evaluating risks to the confidentiality, integrity and availability of PHI or PII based on existing controls and the amount and type of PHI and PII stored, maintained, received or transmitted by the system. The following environments are included:

- TTEC

- TTEC Digital
- Any organization that TTEC has completed an acquisition of, no sooner than one year after the acquisition

As a result of these risk assessments, the CISO and the application owner will determine and document the sensitivity of the application.

*Evaluating Risk after Serious Security Incidents*

As set forth in the Company's Notification of Possible Security Incidents and Breaches Policy, the Company will take steps to mitigate harm resulting for incidents and breaches and to prevent similar incidents or breaches from occurring in the future. The Chief Privacy Officer or the Chief Information Security Officer (CISO) is responsible for mitigation efforts depending on the nature of the incident or breach. Based on the nature and severity of the security incident, the CISO may require an additional risk assessment to be performed as part of the mitigation efforts.

In the event of an identified risk affecting a client environment, TTEC will provide appropriate information to the client and discuss controls to ensure the safety of the respective environment.

*Evaluating Risk Prior to Major Changes to Operations, Applications or Infrastructure*

Global Information Security (GIS) should be engaged prior to making any changes to operations, applications or infrastructure. GIS will evaluate the change and provide guidance on mitigating information security risk associated therewith. The objective is to mitigate risk to an acceptable level as approved by management while meeting the business need. Depending on the nature of the change, the CISO may require an additional risk assessment be performed.

*Periodic Assessment of Controls*

The Company periodically assesses a subset of controls defined in the NIST Cybersecurity Framework. GIS is responsible for these efforts.

*Assessment of Loss of Network Services*

The CISO and relevant stakeholders will evaluate the impact of the loss of network service to the business.

*Regular Review of Risk Assessments*

The risk assessments should be reviewed at least annually by the IT Steering Committee. Risk assessments will be maintained and tracked by GIS.

*Risk Mitigation and Corrective Action for Risks and Nonconformities*

Risk Treatment Plan

The Company will develop a risk treatment plan that includes risks and nonconformities identified by the Company during continuous risk monitoring. The plan will contain corrective actions and mitigations, including any that are developed as a result of the Company's enterprise and information systems risk assessments. The risk treatment plan must be reviewed and updated at least quarterly to monitor the Company's progress on corrective actions.

Strategic Planning

The risk assessment results and risk treatment plan will be distributed to the Healthcare Compliance Committee and the IT Steering Committee after the results have been compiled. The results should be used by departments when planning for the subsequent year, including in making budget decisions and setting department goals.

## III. DEFINITIONS

**Covered Entity** – A health care provider, a health care payer or a health care clearinghouse. Health care providers include doctor's offices and hospitals. Health care payers include health insurance companies. All Company clients that sell or provide health care insurance are Covered Entities for the purposes of this policy.

**Impact** – The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure, modification, destruction or loss of information or information systems availability.

**Protected Health Information (PHI)** – Any information received from or created on behalf of a Covered Entity about (i) health status, (ii) the provision of health care, or (iii) the payment for health care that can be linked to a specific individual. Examples of PHI include insurance policy information, the insurance application and information related to treatment or payment for treatment.

**Personally Identifiable Information (PII)** – A (i) Social Security number; (ii) driver's license number or other government identifier; (iii) account number, credit card number or debit card number whether or not combined with any security code, access code, or password; (iv) medical information; (v) email address or user name together with the password or password recovery security question; (vi) an individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual; (vii) name; (vii) date of birth; (ix) mother's maiden name; (x) unique biometric data (i.e. finger print, voice print, retina or iris image); (xi) unique electronic identification number, address or routing code; and (xii) telecommunications access device such as devises, cards, plates, codes, PINs, mobile identification number or similar that can be used to obtain money, goods, services or to initiate a transfer of funds (such as ApplePay or a digital wallet).

**Risk** – The net business impact considering: (i) the probability that a particular threat will exercise a particular vulnerability; and (ii) the resulting impact if this should occur. Risks arise from legal liability or business loss due to: (i) unauthorized disclosure, modification or destruction of information; (ii) unintentional errors or omissions; (iii) IT disruptions due to natural or man-made disasters; and (iv) failure to exercise due care and diligence in the implementation and operation of the IT system.

**Threat** – The potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability

**Vulnerability** – A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach of a violation of the system's security policy.

## IV. APPLICABILITY

This policy applies to all TTEC companies worldwide, including subsidiaries and controlled affiliates, and all acquired companies subject to earn-out provisions, whether or not they trade under the TTEC brand or as part of a different trading platform. It does not apply to Percepta entities.

## V. RESPONSIBILITY

Compliance with this policy is the responsibility of GIS and stakeholders that participate in or are required mitigate risk identified in during risk assessments. The CISO is responsible for policy compliance. Failure to comply with the policy will put TTEC at a substantial risk and may subject the Company and employees to civil and criminal liability (which may include large monetary fines as well as jail time). Violations of the policy, including reporting concerns about corrupt conduct of others, will result in disciplinary action including termination of employment.

## VI. EXCEPTIONS TO THE POLICY

There are no exceptions to this policy.

## VII. RELATED POLICIES AND PROCEDURES

This policy is aligned with other TTEC related policies and procedures, including without limitation:

- Global Information Security Requirements
- Information Security Policy
- Information Security Risk Management SOP

Last revised date: October 06, 2023