

# Security and Privacy Committee Charter

Information in this document is subject to change without notice.

No part of this document may be reproduced or transmitted in any form or by any means, for any purpose, without the express written permission of TEMENOS HEADQUARTERS SA.

© 2019 Temenos Headquarters SA - all rights reserved



## Document History

Author	Version	Date
Emily Walton	v.1.1	22 May 2017
Emily Walton	v.1.2	15 June 2017
Petr Mandik	v.1.3	04 December 2019
Flavien Bau	v.1.4	22 June 2020

Comments:

Reviewed and approved by: Security and Privacy Committee



## Statement of Purpose

As a market –leading software specialist, supplying banks and other financial institutions all over the world with mission critical banking software and solutions, Temenos recognizes that security and data protection are fundamental to its clients, partners and employees. This encompasses security relating to its products and services including its hosted solutions as well as its own information security systems and physical and location security arrangements. In addition, Temenos respects that everyone has rights with regard to how their personal data is handled. Temenos understands that unauthorized use or access to corporate confidential information or personal data can cause serious damage to our clients and our employees.

The purpose of Security and Privacy Committee is to oversee Management's efforts to implement global information security and privacy compliance programs that are aligned with company strategy and support promotion of emerging technologies such as the cloud services or artificial intelligence application. The Committee's role is one of oversight, recognizing that developing a culture of security and awareness of privacy and personal data among all employees is the responsibility of all involved within the organization.

The Security and Privacy committee will *inter alia*:

- Provide business line input and facilitate the development, articulation, implementation and operation of an effective Information Security, Privacy and Compliance Strategy.
- Assist Management and the Board of Directors in establishing an appropriate “tone at the top” and promote a strong culture of awareness of security, data protection and compliance programs throughout Temenos.
- Identify general and specific security, privacy risks and opportunities including those arising from cloud service offering and make decisions which are communicated to the business or escalate to the Executive Committee as appropriate.
- Make recommendations on the measures Temenos will take to achieve the objective of adherence to the security and data protection measures across all business lines including cloud, advising on policies, processes and controls to be developed within the organization as part of the security and data protection arrangements.
- Provide for executive management responsibility over the company introduced security and privacy compliance programs including those that are aimed to address emerging technologies such as the cloud technology.
- Foster a proactive approach to implement and communicate policies related to security, IT, data protection or compliance programs and continue to review such policies as appropriate.
- Act as the point of escalation for managing incidents relating to unauthorized use or access to corporate confidential information or personal data.

## Committee Membership

The membership of the Security and Privacy Committee shall be selected to provide a broad connection across the functions and organizations of Temenos. As such, the Committee members should comprise security and privacy, cloud, product security and corporate function representatives. The Committee shall be chaired by the Chief Information and Security Officer.

The Security and Privacy Committee standing members consists of:

### Security and Privacy

- Chief Information Security Officer acting as Chairman
- Privacy and Security Director
- IT Security and Compliance Manager
- Product Security Director



### Cloud business

- Temenos Cloud Managing Director
- Cloud Security Director
- Associate Legal Counsel, for cloud and data protection issues

### Corporate

- General Counsel
- Chief Human Resources Officer
- Finance Director
- Corporate Social Responsibility Director
- Group Business Continuity and Risk Manager
- Group Head of Internal Audit

Members of the Security and Privacy Committee shall be appointed and may be replaced or removed by the decision of the Committee. Members may voluntarily resign from their position as a Member of the Committee, subject to valid reason. If such case occurs, the Committee will seek for replacement to ensure continuation of relevant business function representation in the committee meetings.

A majority of members of the Security and Privacy Committee will form a quorum. Concurrence of a majority of the quorum is required for actions to be taken. Written minutes shall be kept and maintained by the Committee Secretary for all formal meetings of the Committee.

The Committee may invite to its meetings other members of the Board, members of the Company management or outside experts or such other persons as the Committee deems appropriate.

## Committee Meetings

The Security and Privacy Committee will meet quarterly. Additional meetings may be held when needed (e.g. important projects or initiatives, workload, availability) and extraordinary meetings may be held where urgent circumstances may require (e.g. upon the occurrence of a security incident, or whenever a decision that may affect organization privacy and security strategy shall be made). Any member of the Committee can request call for an extraordinary meeting. Meetings may be held in person or via other methods of connectivity (conference call, phone).

The agenda and supporting documents are where possible to be circulated 24 hours in advance, with any Committee member able to propose to items for the agenda. Minutes will be circulated for comments within a stated timescale after the meeting and then finalized.

## Committee Duties and Responsibilities

The responsibilities of the Security and Privacy Committee include, but are not exclusive to, the following:

- Oversee global security and data protection efforts with the objective of ensuring that Temenos has established written policies, guidelines, operating procedures in compliance with the laws, rules and regulations of countries in which it operates and in accordance with the internationally-recognized industry applicable standards.
- Ensure that the Information Security & Privacy Strategy is informed by, and aligned to the IT Strategy and overall business strategy.
- Review and approve the introduction of new compliance programs, in order to enhance the effectiveness of the overall security and data protection efforts.
- Review significant security incidents reported through all channels relating to security and data protection. Decide on and oversee any remediation or notifications to be carried out.
- Review data collection reports which are relevant to the objective of promoting security and data protection, including statistics relating to the undertaking of mandatory training.



- Review Security & Privacy risk management process and key risks.
- Advise business units on compliance with external regulations, applicable standards and internal policies.
- Review effectiveness and impact of the security, data protection and applicable compliance programs.
- Achieve and maintain a constant state of compliance with relevant standards for applicable platforms and systems (business-as-usual).
- Ensure that critical roles and responsibilities to conduct security, privacy and compliance programs across Temenos business lines including cloud are identified and assigned.
- Ensure reasonable business resiliency and continuity.
- Support the allocation of adequate resources to enable the Company and its employees to comply with the Security and data protection policies.
- Support the allocation of adequate resources and systems for audit.
- Ensure that written policies, guidelines, procedures are reviewed and updated periodically while compliance with applicable international standards is maintained.
- Ensure guidelines and standards are communicated across Temenos through training programs and other communication initiatives and promoting the establishment of local data champions to promote awareness of security and data protection.
- Report at least annually to the Executive Committee/Board of Directors on it's own performance.

Last review: June 2020