# Organization of information security

## Internal organization

*Axiom:* A structured management framework directs, monitors and controls the implementation of information security as a whole within Tellida Pvt Ltd

**NOTE: This is a generic structure chart (organogram). It should be replaced by one describing Tellida Pvt Ltd’s actual management structure for information security. All major components must be described below. The text that follows outlines a generic information security management structure based on ISO 27002 but this should be customized to suit Tellida Pvt Ltd’s specific management hierarchy, rôles and responsibilities.**

### Management commitment to information security

Corporate governance is ultimately answerable to the Board of Directors ("the Board"). Corporate governance includes the management and control of information security issues. In practice, the Board delegated executive duties for most governance issues to the Executive Directors, overseen by the Chief Executive Officer (CEO).

The Executive Directors provide broad strategic guidance by endorsing and mandating information security principles and axioms, but the Security Committee (SC), chaired by the Chief Security Officer, is in charge of operational responsibilities for physical and information security (CSO).

The Executive Directors rely on the SC to coordinate efforts across Tellida Pvt Ltd and ensure that appropriate policies are in place to support the company's security principles and assumptions. To guarantee that the principles, axioms, and policies are followed in practice, the Executive Directors rely on feedback from the SC, CSO, ISM, auditors, Risk Management, Compliance, Legal, and other functions.

The Executive Directors demonstrate their commitment to information security by:

* A statement of support from the CEO;
* Reviewing and re-approving the principles and axioms every year;
* Approving the IT budget including a specific element set aside for information security;
* Receiving and acting appropriately on management reports concerning information security performance metrics, security incidents, investment requests *etc*.

### Information security co-ordination

Information security activities should be co-ordinated throughout Tellida Pvt Ltd to ensure consistent application of the security principles, axioms and policy statements.

The Executive Directors have charged the SC with the task of securing Tellida Pvt Ltd’s assets. The SC is responsible for:

* Management oversight and direction for both physical and logical aspects of security, including information security;
* Coordinating and directing Tellida Pvt Ltd’s entire security framework, including the information security controls at all Tellida Pvt Ltd locations mediated through the Local Security Committees (see below) ;
* Commissioning or preparing information security policy statements, ensuring their compliance with the principles and axioms approved by the Executive Directors, and formally approving them for use throughout Tellida Pvt Ltd;
* Periodically reviewing the security policy statements to ensure the efficiency and effectiveness of the information security controls infrastructure as a whole, recommending improvements wherever necessary;
* Identifying significant trends and changes to Tellida Pvt Ltd’s information security risks and, where appropriate, proposing changes to the controls framework and/or policies for example by sponsoring major strategic initiatives to enhance information security;
* Reviewing serious security incidents and, where appropriate, recommending strategic improvements to address any underlying root causes;
* Periodically reporting on the status of the security controls infrastructure to the Executive Directors, and liaising as necessary with the Risk Management and Audit Committees *etc*., using metrics and other information supplied by the CSO, Local Security Committees, the ISM, Internal Audit and others.

TSome of the SC's tasks are delegated (for example, to the ISM, the Information Security function, and Local Security Committees), but the Executive Directors are responsible for the overall efficacy of information security at Tellida Pvt Ltd.he SC delegates some of its responsibilities (for example to the ISM, the Information Security function and Local Security Committees) but remains accountable to the Executive Directors for the overall effectiveness of information security throughout Tellida Pvt Ltd.

Business units or locations within Tellida Pvt Ltd have **Local Security Committees (LSCs)** which report to the SC. LSCs are responsible for:

* Providing strategic guidance, assistance, and resources to manage all types of local security challenges and, as a result, ensuring that Tellida Pvt Ltd's information assets are effectively and consistently protected;
* coordinating and exchanging information to ensure that the information security policy manual is followed consistently throughout all Tellida Pvt Ltd sites;
* Identifying and identifying certain Significant Information Assets, as well as appointing competent Information Asset Owners (IAOs) for them;
* Obtaining metrics and other data on the overall effectiveness of information security controls within their remit and reporting to the SC.

### Allocation of information security responsibilities

The Executive Directors have appointed a **Chief Security Officer (CSO)**. The **CSO** is responsible for:

* Chairing the SC;
* Taking the lead on overall information governance, for example, by releasing the policy manual and providing the overall strategic direction, support, and evaluation required to ensure that information assets are identified and appropriately protected throughout Tellida Pvt Ltd;
* The ISM and Information Security Management teams are appointed and managed.

#### The **ISM** and **Information Security Management** are responsible for:

* Defining information security standards, methods, and recommendations, including technical and non-technical;
* Supporting IAOs and managers in defining and implementing controls, processes, and supporting tools in order to comply with the policy manual and manage information security risks;
* Examining and monitoring policy statement compliance, as well as participating in internal audit and control self-assessment (CSA) processes;
* Information security metrics and incidents are collected, analyzed, and commented on.
* assisting IAOs with the investigation and correction of information security events and other policy infractions;
* When applicable, liaising with related internal departments such as IT Operations, Risk Management, Compliance, and Internal Audit, as well as the CSO, LSCs, and SC, and external functions such as the Police;
* Organizing a security awareness program for employees in order to improve security culture and establish a comprehensive grasp of ISO/IEC 27002 requirements.

#### **Managers** throughout Tellida Pvt Ltd are responsible for:

* Implementation of the information security policy manual on a daily basis;
* Assuring that appropriate technical, physical, and procedural controls are in place, and that they are correctly applied and used by all personnel, in accordance with the handbook. They should, in particular, take steps to guarantee that workers are safe.:
* Comply with the policy statements and actively support the accompanying controls; and Are informed of their responsibility to meet applicable corporate policy statements by suitable awareness, training, and education efforts.
* Are observed for compliance with the policy statements and the proper operation of the accompanying controls, and are reminded of their responsibilities as needed;
* Providing the necessary guidance, resources, assistance, and oversight to ensure that information assets are properly secured within their sphere of influence;
* Informing Information Security Management and/or IAOs of actual or suspected policy violations (information security incidents) affecting their assets; and Evaluating policy axiom compliance through the CSA process and periodic Internal Audits.

**Information Asset Owners** (IAOs) are managers held accountable by their LSC or the SC for the protection of specific Significant Information Assets? IAOs may assign information security tasks to managers or other personnel, but they are still responsible for ensuring that the activities are completed correctly. IAOs are in charge of:

* Appropriate information asset classification and protection;
* determining and funding appropriate protective controls;
* Authorizing access to data assets based on classification and business requirements;
* [For the creation of new application systems] Conducting or commissioning information security risk assessments to ensure that information security needs are well established and documented early in the development process;
* ensuring that regular system/data access reviews are completed on time; and monitoring compliance with asset protection regulations.

**All Tellida Pvt Ltd workers** When it comes to their jobs, they are accountable for adhering to the information security policy manual's concepts, axioms, and policies. They are in charge of ensuring the security of the data entrusted to them. Each employee agrees to follow Tellida Pvt Ltd's information security rules as a condition of employment upon hire. Any employee who fails to follow the security policies could face disciplinary action, which could include termination of employment or contract, as well as criminal prosecution.

**Exemptions process:** For an information asset under their remit, an IAO may suggest exclusions to principles, axioms, or policy statements stated in the policy manual. The ISM is in charge of examining the risks caused by the proposed exemptions and, in most circumstances, recommending mitigating procedures to reduce those risks. Proposed exemptions that the ISM believes could have a substantial impact on Tellida Pvt Ltd's information security risks may be forwarded to the LSC, SC, CSO, and/or Executive Directors for approval, depending on the severity of the perceived risk. Exemptions are not indefinite, so a program (action plan) is usually necessary to assure complete compliance with the within a set time frame. The IAO will be held responsible for the mitigating controls and action plan, and will be responsible for any increased risk associated with the policy exemption and mitigating controls until the exemption is resolved.

The SC, LSCs, CSO, and ISM must examine current exemptions at least once a year. Authorized exemptions must be listed in an annual status report to the Executive Directors, the reasons for policy exemptions must be clarified, and plans to resolve non-compliance with policy (typically through strategic investment to achieve compliance, or by changing the policy) must be explained.