ISO 27001:2022 SCOPE DOCUMENT TEMPLATE

DEFINING BOUNDARIES FOR INFORMATION SECURITY EXCELLENCE

Prepared by :
NIRANJAN V

ISO 27001:2022 Information Security Management System

Scope Document

Departments in Scope of ISO 27001:2022

The Information Security Management System and related controls are designed and implemented in the following departments within <Organization Name>:

Department Name	Function
DevOps	The DevOps Team manages infrastructure through code-based tools, ensuring scalability and efficiency in cloud environments
Product Development	The Product Development Team is responsible for conceptualizing, designing, and creating new products or improving existing ones.
Customer Support	The Customer Support Team handles inquiries, complaints, and feedback, striving to ensure customer satisfaction and loyalty. Customer Service manages various communication channels, such as phone, email, chat, and social media, to promptly address customer needs.
Quality Assurance	The QA Team develops and implements testing strategies, methodologies, and processes to identify defects and prevent issues before deployment. They conduct rigorous testing, including functional, regression, performance, and security testing, to verify that products meet specified requirements and standards.

Interface Departments in Scope of ISO 27001:2022

Some of the Business functions / departments / teams which are not in direct scope of ISO 27001:2022, may have an impact on the security and functioning of <Organization Name>'s ISMS. These departments need to be

treated as interfaces and protected as part of the ISMS; vendors, partner companies, regulators and customers are outside the scope of ISMS.

Department Name	Function
Human Resource	The HR Team oversees recruitment and hiring processes, including sourcing candidates, conducting interviews, and onboarding new employees. HR handles employee relations, including performance management, disciplinary actions, and conflict resolution.
Information Technology (IT)	The IT (Information Technology) Team is responsible for managing the organization's technology infrastructure and systems. They oversee the implementation, maintenance, and security of hardware, software, and networks.
Admin and Physical Security	The Admin and Physical Security Team is responsible for managing and maintaining the physical security of the organization's facilities, assets, and personnel. They oversee access control systems, surveillance cameras, and security guards to safeguard against unauthorized access and protect sensitive areas.
Infosec and Compliance	The Infosec (Information Security) and Compliance Team is responsible for safeguarding the organization's information assets and ensuring compliance with relevant laws, regulations, and standards. They develop and enforce information security policies, procedures, and controls to protect against cybersecurity threats, such as unauthorized access, data breaches, and malware attacks.
Finance	The Finance Team is responsible for managing the organization's financial resources, processes, and reporting. They oversee budgeting, forecasting, and financial planning to support strategic decision-making and ensure financial sustainability. Finance professionals manage accounts payable and receivable, ensuring timely

	payment of invoices and accurate recording of transactions.
Legal	The Legal department is responsible for managing legal affairs and ensuring compliance with applicable laws and regulations. They provide legal counsel and advice to the organization on various matters, including contracts, employment law, intellectual property rights, and corporate governance. Legal professionals draft, review, and negotiate contracts and agreements to protect the organization's interests and minimize legal risks.

Dependencies in Scope of ISO 27001:2022

<Organization Name> is dependent on Vendors/Third parties/Service Providers for several critical ISMS related processes, viz. data storage, internet access provision, background-verifications etc. They play a key role in the operations of the <Organization Name>. They are dependencies to the <Organization Name>'s ISMS; but will not come under the direct scope of ISMS.

Dependencies	Function
Cloud Service Provider	The <Organization Name> depends on the cloud service provider to maintain the security and availability of their data and systems. This includes ensuring that the provider implements robust data security measures, complies with relevant security standards and certifications, adheres to contractual agreements outlining security responsibilities, and promptly responds to security incidents or breaches.
Background Verification Vendor	The <Organization Name> depend on the vendor to conduct thorough and accurate verification processes while safeguarding the privacy and integrity of personal data. This includes ensuring that the vendor implements appropriate security measures to protect against unauthorized access, data breaches, and misuse of information.

Contractors	The <Organization Name> depend on contractors to maintain confidentiality, integrity, and availability of data and systems during their engagement. This includes ensuring that contractors comply with security requirements outlined in contracts, adhere to relevant security standards and regulations, and implement appropriate security controls to mitigate risks.
Service Providers	The <Organization name> depend on service providers to maintain the confidentiality, integrity, and availability of data and systems related to the services they provide. This includes ensuring that service providers comply with contractual security requirements, adhere to relevant industry standards and regulations, and implement appropriate security controls to mitigate risks.

Locations in Scope of ISO 27001:2022

Scope of ISMS is limited to <Organization Name> business operations that are carried out from the below location:

Location	Address
Bangalore	1234, 5th Cross Road, Indiranagar, Bangalore, Karnataka, India 560038
Chennai	456, Anna Salai, Teynampet, Chennai, Tamil Nadu, India 600018
Mumbai	789, Hill Road, Bandra West, Mumbai, Maharashtra, India 400050
New Delhi	101, Main Road, Connaught Place, New Delhi, Delhi, India 110001

The Functions (Departments, Interfaces and Dependencies) in Scope of ISO 27001:2022 at Bangalore would be:

- Customer Support
- QA
- Human Resource
- Admin & Physical Security
- Information Technology (IT)

- Cloud Service Provider
- Background Verification Vendor
- Service Providers

The Functions (Departments, Interfaces and Dependencies) in Scope of ISO 27001:2022 at Chennai would be:

- DevOps
- Product Development
- QA
- Human Resource
- Admin & Physical Security
- Information Technology (IT)
- Cloud Service Provider
- Background Verification Vendor
- Service Providers
- Contractors

The Functions (Departments, Interfaces and Dependencies) in Scope of ISO 27001:2022 at Mumbai would be:

- QA
- Human Resource
- Admin & Physical Security
- Information Technology (IT)
- Infosec and Compliance
- Cloud Service Provider
- Background Verification Vendor
- Service Providers
- Contractors

The Functions (Departments, Interfaces and Dependencies) in Scope of ISO 27001:2022 at Delhi would be:

- DevOps
- Product Development
- Human Resource
- Admin & Physical Security
- Information Technology (IT)
- Legal
- Finance
- Infosec and Compliance
- Cloud Service Provider

- Background Verification Vendor
- Service Providers
- Contractors

ISO 27001:2022 Scope Statement

Management of information security for provisioning of <Organization Name> service lines delivered by DevOps, Product Development, Customer Support and Quality Assurance with support from Human Resource, Information Technology (IT), Admin and Physical Security, Infosec and Compliance, Finance and Legal and dependent on Cloud Service Provider, Background Verification Vendor, Contractors and Service Providers.

The Information Security Management System (ISMS) applies in accordance with Statement of Applicability (SOA) v1.0 released on <date>.

Exclusions from ISO 27001:2022 Scope

- All operations and business functions (other than what is mentioned as 'In scope' in this document)
- External Parties: Customers, Competitors, Regulators, Media, Vendors / Third parties

Stay Informed, Stay Secure With Daily InfoSec Wisdom

REACH OUT FOR ISO 27001 MENTORING AND GUIDANCE

Let's build a stronger infosec community and grow together

Prepared by :
NIRANJAN V