

Security Roles and Responsibilities

Owner	[Security owner role]
Approved by	[Policy approver role]
Effective date	[Effective date]
Next review	[Next review date]
Version	1.0

1. Purpose and scope

This document defines who at [Company name] (the "Company") is responsible for each part of the information security program, so that every control has an owner and nothing depends on an assumption. It covers the Company's product, the infrastructure in the production cloud environment, corporate systems, and the people who use them.

At a company of this size one person often holds more than one role. That is acceptable, provided each role has a named holder and no one approves their own access or reviews their own work.

2. Roles

Role	Held by	Core responsibilities
Executive sponsor	[Policy approver role]	Sets the tone for security, approves policies and risk acceptance, provides resources, and receives security reporting at least twice a year.
Security and compliance owner	[Security owner role]	Runs the security program day to day: maintains policies, runs risk assessments and access reviews, leads incident response, manages the audit, and tracks remediation.
Engineering lead	[Engineering owner role]	Owns the security of the Company's product and the production cloud environment: secure development, change management, vulnerability remediation, logging, backups and recovery.
IT lead	[IT owner role]	Owns corporate systems and devices: account provisioning and removal, device encryption and updates, endpoint protection, and SaaS administration.

Role	Held by	Core responsibilities
People lead	[People owner role]	Owns the people side of security: background checks, onboarding and offboarding notices, policy acknowledgments, training records and disciplinary process.
All personnel	Everyone	Follow Company policies, complete training, protect credentials and data, and report suspected incidents within 1 hour.

3. Responsibility matrix

R = Responsible (does the work). A = Accountable (owns the outcome and signs off; exactly one per activity). C = Consulted (gives input before the work is done). I = Informed (told of the result).

Activity	Frequency	Executive	Security owner	Engineering	IT	People
User access reviews	Quarterly	I	A	R	R	I
Onboarding and offboarding of accounts	Each joiner and leaver	I	A	R	R	R
Vendor security reviews	At onboarding, then yearly	I	A, R	C	C	I
Incident response	Each incident	C	A, R	R	R	C
Policy approval	Yearly	A	R	C	C	C
Risk assessment	Yearly and on major change	A	R	C	C	C
Vulnerability remediation	Continuous, to set timelines	I	A	R	R	I
Backup restore testing	At least yearly	I	A	R	I	I
Security awareness training	At hire and yearly	I	A, R	C	I	R

Where one person holds two roles in the same row, a different person performs the review or approval. For access reviews, no one reviews their own access; the [Policy approver role] reviews the access of the security owner.

4. Named role holders

Write the name of the person who holds each role today and a deputy who acts when they are unavailable. Update this table within 5 business days of any change.

Role	Name	Deputy	Date assigned
Executive sponsor			
Security and compliance owner			
Engineering lead			
IT lead			
People lead			

5. Changes and review

When a role holder leaves or changes role, the [Policy approver role] assigns a new holder before their last day, and the outgoing holder hands over open actions in writing. The [Security owner role] reviews this document at least once a year and after any change to the team structure. The [Policy approver role] approves each new version.

6. Acknowledgment

I accept the security role assigned to me in this document. I understand the responsibilities of that role and my part in the responsibility matrix, and I will tell the [Security owner role] if I can no longer carry them out.

Role holder

Name:

Signature:

Date:

Source

Source: free template from www.polaralabs.com/templates/security-roles-and-responsibilities (CC BY 4.0).