

Users, Roles, Responsibilities & Training

Status	ACTIVE
Owner	@Jonas Purtschert
Last update	20 Feb 2025

Table of Contents [↗](#)

1. [Introduction](#)
2. [Technical Users](#)
3. [Internal Users](#)
 1. [Internal Role Descriptions](#)
 1. [Sysadmin](#)
 2. [Developer](#)
 3. [Member of Management](#)
 4. [Customer Success Employee](#)
 2. [Internal Role Management](#)
4. [External \(Platform\) Role Descriptions](#)
 1. [Team User](#)
5. [Training of Employees](#)
 1. [For Internal Use only, DO NOT PUBLISH](#)
6. [Table of Members](#)

Introduction [↗](#)

This file outlines the roles and responsibilities of our organization's members and the roles of the users. Roles and responsibilities in our organization are assigned on a Need-to-Know basis.

Technical Users [↗](#)

Technical users are always restricted to the minimal permission set that is needed to fulfil it's designed purpose.

Technical Users can only be managed by the Sysadmin internal Role.

Internal Users [↗](#)

Internal users are never shared users and always require 2 factor authentication.

The permissions of internal users are reviewed every three months and permissions that are no longer required to fulfil their role are revoked.

Internal Role Descriptions [↗](#)

Sysadmin [↗](#)

Sysadmins manage the IT infrastructure of our organization. In order to carry out their work, they have full access to any application, database, infrastructure component of our organizations cloud platform.

Developer

Developers have access to the codebase, can push new code to the codebase & trigger deployments to integration & production environments.

Member of Management

Members of the management of our organization. They can read/modify Microsoft User permissions and have elevated permissions on the Administration UI.

Customer Success Employee

Employees that need access to the Administration UI. They can see the companies, teams & employees that use our Platform. They can also log in as an administrative Employee and manage Platform Settings for teams.

Internal Role Management

Internal roles are assigned to employees of Moodtalk in two ways:

1. Via Microsoft Entra ID by a Sysadmin or a Member of Management
2. Via Keycloak by a Sysadmin

External (Platform) Role Descriptions

User roles are assigned by Moodtalk Staff with the Roles “Member of Management”, “Sysadmin” or “Customer Success Employee” and are not imported.

Team User

A user can be assigned to one or multiple teams. The user can manage their teams and use the team specific functionality of Moodtalk.

Division User

A user can be assigned to one or multiple divisions. The user can manage their divisions and use the division specific functionality of Moodtalk.

Company User

A user can be assigned to one or multiple companies. The user can manage their companies and use the company specific functionality of Moodtalk

Training of Employees

Moodtalk Employees receive a yearly internal cybersecurity training. The training is a comprehensive program designed to equip staff with essential knowledge and skills to protect the organization’s digital assets. It covers key areas such as recognizing phishing scams, using strong and unique passwords, secure handling of sensitive information, and the importance of two-factor authentication. Employees will learn best practices for safeguarding devices, securing home networks when working remotely, and avoiding malware. The training also addresses compliance with data protection regulations.