Vmobile IT Password Policy and Guidelines

Contents

[Version History 1](#_Toc205972922)

[Purpose & Scope 1](#_Toc205972923)

[Overview of Password Security at Vmobile 1](#_Toc205972924)

[Applicability of This Policy 2](#_Toc205972925)

[Policy Summary 3](#_Toc205972926)

[Password Change Schedule 3](#_Toc205972927)

[Regular Password Change Intervals 3](#_Toc205972928)

[Situations Requiring Immediate Password Change 4](#_Toc205972929)

[Password Reset Reasons: Annual Breakdown 4](#_Toc205972930)

[Password Creation Guidelines 5](#_Toc205972931)

[Best Practices 5](#_Toc205972932)

[Do’s and Don’ts for Password Creation 5](#_Toc205972933)

[Password Requirement Checklist 6](#_Toc205972934)

[Reset & Recovery Process 6](#_Toc205972935)

[Overview of Password Reset Requests 7](#_Toc205972936)

[Step-by-Step Instructions for Requesting a Password Reset 7](#_Toc205972937)

[Expected Response Times and Support Availability 8](#_Toc205972938)

# Version History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Summary of Changes** |
| 1.0 | 2024-06-10 | HR & IT Admin | Initial release: established baseline HR and IT policies. |
| 1.1 | 2024-06-18 | HR Manager | Updated onboarding procedures and clarified leave policies. |
| 1.2 | 2024-06-25 | IT Director | Added password management requirements and device usage rules. |
| 1.3 | 2024-07-02 | HR & IT Admin | Incorporated remote work guidelines and data privacy updates. |
| 1.4 | 2024-07-10 | HR Manager | Revised employee conduct section; added escalation protocols. |

# Purpose & Scope

## Overview of Password Security at Vmobile

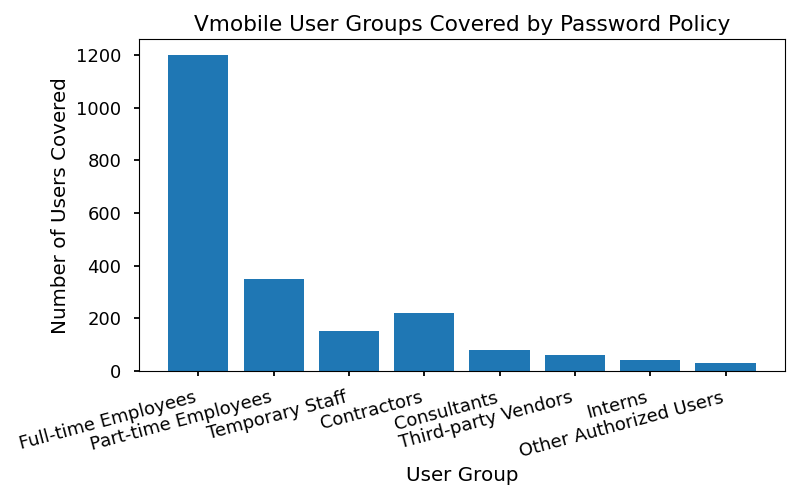
At Vmobile, safeguarding our telecom systems and sensitive customer data is a top priority. Strong password practices are fundamental to our overall cybersecurity strategy, as passwords serve as the first line of defense against unauthorized access to our networks, applications, and databases. Weak or compromised passwords can lead to data breaches, service disruptions, financial losses, and erosion of customer trust. By enforcing robust password policies, Vmobile ensures the confidentiality, integrity, and availability of our information assets, while meeting regulatory and contractual obligations in the telecommunications sector.

## Applicability of This Policy

This Password Policy applies to all individuals who access Vmobile’s information systems, including but not limited to:

* Full-time and part-time employees
* Temporary staff
* Contractors
* Consultants
* Third-party vendors
* Interns
* Any other authorized users of Vmobile’s IT infrastructure

Compliance with this policy is mandatory for anyone granted access to Vmobile’s internal and external systems, including workstations, mobile devices, cloud platforms, and web-based applications. Failure to adhere to these requirements may result in disciplinary action, up to and including termination of access or employment, in accordance with Vmobile’s HR and IT security protocols.



|  |  |  |
| --- | --- | --- |
| **User Group** | **Examples** | **Access Level** |
| Employees | Staff, managers, executives | Full/Departmental |
| Contractors | IT support, project-based | Limited/Project |
| Vendors | Software partners | System-specific |
| Interns | Student placements | Restricted |
| Consultants | Security, compliance experts | Temporary/Advisory |

All users must familiarize themselves with the requirements outlined in this policy and participate in periodic security awareness training as scheduled by Vmobile’s HR and IT departments.

# Policy Summary

Vmobile’s Password Policy is designed to safeguard company data, systems, and employee accounts by enforcing robust password practices. All employees are required to adhere strictly to the following standards:

* Minimum password length: 12 characters
* Required character types: Uppercase letters, lowercase letters, numbers, and special symbols
* Prohibited password reuse: Employees may not reuse any of their previous five passwords
* Account lockout limits: After 5 consecutive failed login attempts, user accounts will be temporarily locked for 30 minutes

# Password Change Schedule

Vmobile is committed to maintaining the highest standards of information security and employee accountability. As part of our ongoing efforts to safeguard company data, all employees are required to adhere to Vmobile’s Password Change Schedule. This policy outlines the mandatory intervals for password updates and specifies situations where immediate action is necessary. Compliance with these guidelines is essential for protecting our systems, customer information, and proprietary business data.

## Regular Password Change Intervals

All Vmobile employees must change their passwords for corporate systems—including email, intranet, CRM, and HR portals—at least once every 90 days. This interval is enforced by automated prompts from our IT systems. Employees will receive reminders via email and system notifications two weeks prior to the expiration of their current password.

Passwords must meet Vmobile’s complexity requirements, which include:

* Minimum length of 12 characters
* At least one uppercase letter, one lowercase letter, one number, and one special character
* No reuse of the previous 5 passwords

Failure to update passwords within the required timeframe will result in automatic account lockout. Employees must contact the IT Helpdesk to regain access.

## Situations Requiring Immediate Password Change

In addition to the scheduled 90-day change, employees must immediately update their passwords in the following situations:

* Suspected or confirmed account compromise
* Loss or theft of a device containing company credentials
* Change in job role or department
* Termination of employment (initiated by HR and IT)
* Unauthorized access attempt detected by IT Security
* Notification from IT regarding system vulnerability

## Password Reset Reasons: Annual Breakdown

|  |  |
| --- | --- |
| **Reason for Password Reset** | **Percentage (%)** |
| Scheduled 90-Day Change | 63 |
| Suspected Compromise | 14 |
| Role Change | 10 |
| Device Loss/Theft | 6 |
| Termination | 5 |
| Unauthorized Access Attempt | 2 |

All employees are expected to remain vigilant and proactive in protecting their credentials. Non-compliance with Vmobile’s Password Change Schedule will be subject to disciplinary action as outlined in the Employee Handbook. For questions or assistance, contact the IT Helpdesk at helpdesk@vmobile.com or extension 2222.

# Password Creation Guidelines

Vmobile is committed to maintaining the security and integrity of our digital assets and systems. As part of our ongoing efforts, all employees are required to adhere to Vmobile’s Password Creation Guidelines when accessing company resources, including workstations, email, cloud services, and internal applications. These guidelines are designed to safeguard sensitive information and prevent unauthorized access.

## Best Practices

When creating passwords for any Vmobile system, employees must prioritize security while ensuring passwords remain memorable. The following practices are mandated by Vmobile’s IT and HR departments:

Passwords must not contain easily guessable personal information, such as birthdays, names, employee ID numbers, or commonly known facts about you.

Employees are encouraged to use passphrases—combinations of random words or a sentence that is easy to remember but hard to guess (e.g., “BlueCar!Swims#River2024”).

Passwords should be unique to Vmobile systems and never reused from other personal or professional accounts.

Avoid using dictionary words, sequential characters (“123456”, “abcdef”), or simple patterns (“qwerty”, “password”).

Consider using a mix of unrelated words, numbers, and symbols to construct a memorable but secure password.

Employees may use password managers approved by Vmobile IT to generate and store complex passwords securely.

### Do’s and Don’ts for Password Creation

* **Do’s:**
* Do create passwords with a minimum of 12 characters.
* Do include uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and special symbols (e.g., !, @, #, $, %, &).
* Do use a passphrase or a combination of random words and symbols.
* Do change your password every 90 days, or immediately if you suspect compromise.
* Do use Vmobile’s approved password manager for storing passwords securely.
* Do verify password strength using Vmobile’s internal password-check tool before finalizing.
* **Don’ts:**
* Don’t use any part of your name, username, or date of birth.
* Don’t use simple sequences or repeated characters (e.g., “111111”, “abcdefg”).
* Don’t reuse passwords across different Vmobile accounts or external sites.
* Don’t share your password with anyone, including Vmobile colleagues.
* Don’t write passwords down or store them in unsecured locations (e.g., sticky notes, unencrypted files).
* Don’t use passwords that have appeared in known data breaches (Vmobile IT will notify if detected).

## Password Requirement Checklist

All passwords created for Vmobile systems must meet the following requirements. Failure to comply may result in restricted access and disciplinary action.

|  |  |
| --- | --- |
| **Requirement** | **Description** |
| Minimum Length | 12 characters |
| Uppercase Letter | At least 1 (A-Z) |
| Lowercase Letter | At least 1 (a-z) |
| Numeric Character | At least 1 (0-9) |
| Special Symbol | At least 1 (e.g., !, @, #, $, %, &, \*) |
| Personal Information Exclusion | Must not contain personal info (name, DOB, employee ID, etc.) |
| Password Reuse | Must not reuse previous 5 passwords |
| Change Frequency | Every 90 days |
| Password Manager Use | Only Vmobile-approved tools permitted |
| Password Leak Monitoring | Must respond to IT alerts for compromised passwords |

Employees are required to review and comply with these guidelines during onboarding and whenever prompted by the Vmobile IT department. For questions or clarifications, contact the Vmobile IT Helpdesk or HR representative.

# Reset & Recovery Process

The following policy outlines Vmobile’s official process for employees to request password resets and recover access to company systems. Vmobile is committed to maintaining secure and reliable access to all digital resources. Adherence to this process is mandatory for all employees.

## Overview of Password Reset Requests

Vmobile employees who experience difficulty accessing their accounts, or who suspect their credentials have been compromised, must promptly initiate a password reset request. The password reset and recovery process is managed exclusively by Vmobile’s IT Helpdesk team to ensure security and compliance. Employees are not permitted to reset their own passwords for core systems outside of the procedures described below.

## Step-by-Step Instructions for Requesting a Password Reset

Employees must follow these steps to request a password reset:

1. **Contact the IT Helpdesk**

* Submit a request via the official IT Helpdesk portal (https://helpdesk.vmobile.com), or
* Call the IT Helpdesk directly at extension 7000 during business hours (Monday–Friday, 8:00 AM–6:00 PM).

2. **Provide Required Information**

* State your full name and employee ID.
* Specify the system or account requiring a password reset (e.g., Vmobile Email, HR Portal, Salesforce).
* Briefly describe the issue (e.g., forgotten password, suspected compromise).

3. **Identity Verification**

* Be prepared to answer security questions based on your HR profile (e.g., date of hire, department, manager’s name).
* If in-person, present your Vmobile employee badge.
* For remote requests, be available for a video verification if prompted.

4. **Password Reset and Recovery**

* Upon successful verification, the IT Helpdesk will reset your password and send a temporary password to your registered Vmobile email address.
* You must log in and change the temporary password within 24 hours.
* If unable to access your email, alternative arrangements (such as SMS or phone call) will be made by IT.

5. **Post-Reset Actions**

* Review recent account activity for unauthorized access.
* Immediately report any suspicious activity to IT Security at security@vmobile.com.

## Expected Response Times and Support Availability

Vmobile IT Helpdesk aims to respond to password reset requests promptly to minimize disruption:

* **Standard Response Time:** Within 1 hour during business hours (Monday–Friday, 8:00 AM–6:00 PM).
* **After-Hours Support:** Limited support available via email (helpdesk@vmobile.com); expect response within 4 hours.
* **Critical Incidents:** For urgent security concerns, mark your request as "Urgent" in the Helpdesk portal or call extension 7777 for immediate escalation.

Employees are reminded that repeated failed login attempts may result in temporary account lockout for security reasons. If locked out, follow the same reset process. All password resets1 are logged and monitored in accordance with Vmobile’s IT security policies.

1For any questions about the reset and recovery process, contact the IT Helpdesk (ithelpdesk@vomobile.com)