9. Account Management and Security Settings (Account)

Overview
This document describes how customers can manage their personal information, passwords, saved addresses, and privacy settings. It also outlines best practices for maintaining account security and complying with data protection standards such as the Information Technology (Reasonable Security Practices and Procedures) Rules, 2011.

9.1 Managing Personal Information

Customers can update their details through the **Account Settings** section on the website or mobile app. Editable fields include:

- Name, phone number, and date of birth
- Shipping and billing addresses
- Preferred language and communication preferences

Changes take effect immediately after confirmation. For security, sensitive details like registered email or phone number require **OTP verification** before saving.

Steps:

1. Navigate to *Account → My Profile → Edit Details.*
2. Update desired fields and click **Save Changes.**
3. Enter the verification code sent to your email or phone to confirm.

9.2 Password and Login Security

Resetting Your Password

If you forget your password:

1. Click **Forgot Password** on the login screen.
2. Enter your registered email or mobile number.
3. Follow the password reset link sent to your email (valid for 30 minutes).

Passwords must meet the following requirements:

- Minimum 8 characters
- At least one uppercase letter, one number, and one special character
- Cannot repeat the previous 5 passwords

Two-Factor Authentication (2FA)

You can enable 2FA under *Account → Security Settings → Two-Factor Authentication*.
Once activated, every login attempt from a new device requires:

- Your account password, and
- A 6-digit OTP sent via SMS or email

This adds an extra layer of security to protect your data.

9.3 Linked Accounts and Third-Party Sign-Ins

Customers can link or unlink third-party logins such as:

- **Google Account**
- **Apple ID**
- **Facebook Login**

Linked accounts simplify login and checkout but can be managed anytime from *Account → Connected Apps*.
When unlinking, customers must set a standalone password before sign-out to avoid being locked out.

9.4 Address and Payment Management

- Add or edit multiple **shipping addresses** for faster checkout.
- Save up to **three payment methods** (cards or wallets) for convenience.
- Card details are tokenized and encrypted using **PCI DSS-compliant** systems — the full card number is never stored.
- Wallets and UPI IDs can be deactivated under *Payments → Manage Wallets*.

Note: For security, saved payment information is automatically purged if not used for 12 months.

9.5 Privacy and Data Settings

Customers can control how their personal data is used under *Account → Privacy Dashboard.*
Options include:

- Downloading a copy of all stored personal data (exportable JSON format).
- Deleting specific saved preferences or browsing history.
- Opting out of personalized recommendations or ad tracking.

If you wish to delete your account:

1. Go to *Privacy Dashboard → Delete Account.*
2. Confirm your password and verify OTP.
3. Your account will be permanently deleted within **7 days** after verification.

During this period, users can cancel the deletion request.

9.6 Security Notifications and Alerts

Customers receive automatic alerts for:

- Password changes
- Login attempts from new devices or locations
- Linked account sign-ins
- Payment method updates

If any of these actions were unauthorized, immediately visit **Help Center → Account Security** to lock your account temporarily.

9.7 Best Practices for Account Security

- Never share OTPs or passwords with anyone.
- Avoid logging in on public or shared computers.
- Review linked devices periodically and remove unused sessions.
- Update your password at least once every 90 days.

9.8 Customer Support for Account Issues

Support Channels

- **Email:** accounthelp@company.com
- **Helpline:** 1800-000-000 (8 AM – 8 PM)
- **Chat:** Available under Help → "Account & Login Issues"

For data-related concerns, customers can contact the **Data Protection Officer (DPO)** at **privacy@company.com.**