

# Admin Account Usage Policy

v1.0 · Reviewed Jun 2026 · Next review Jun 2027

---

HALVED LIMITED

---

## ADMINISTRATIVE ACCOUNT USAGE POLICY

Version: 1.0 Effective Date: 4th June 2026 Last Review: 4th June 2026 Next Review: 4th June 2027

Owner: Andrew James, CEO

### 1. PURPOSE

---

This policy defines how administrative accounts must be used at Halved Limited to maintain security and comply with Cyber Essentials requirements.

### 2. SCOPE

---

This policy applies to all users with administrative access to Halved systems, including:

- macOS devices
- Microsoft 365 / Azure
- GitHub
- MongoDB Atlas
- Cloudflare
- Other cloud services requiring administrative access

### 3. POLICY REQUIREMENTS

---

#### 3.1 Separate Admin Accounts

Every user requiring administrative access **MUST** have two separate accounts:

- Standard Account: For daily work (email, messaging, browsing, coding, collaboration)
- Admin Account: ONLY for administrative tasks (installing software, changing system configurations, creating/deleting accounts, modifying security settings)

### 3.2 Admin Account Naming Convention

- macOS: andrew-admin (local account)
- Cloud services: [andrew-admin@halved.io](mailto:andrew-admin@halved.io)

### 3.3 Prohibited Activities on Admin Accounts

Admin accounts must NOT be used for:

- Sending or receiving email
- Web browsing
- Messaging (Slack, Teams, WhatsApp, etc.)
- Writing code or documents
- Any daily work activities

### 3.4 Permitted Activities on Admin Accounts

Admin accounts may ONLY be used for:

- Installing or uninstalling software
- Changing system configurations
- Creating or deleting user accounts
- Modifying security settings
- Performing system updates
- Other explicitly administrative tasks

### 3.5 Admin Account Session Management

- Log into admin account only when performing an admin task
- Log out immediately after the task is complete
- Do not leave admin accounts logged in

- Maximum admin session duration: 30 minutes

### 3.6 Admin Account Security

- All admin accounts MUST have multi-factor authentication (MFA) enabled
- Admin account passwords must be at least 12 characters
- Admin account passwords must be unique (not shared with any other account)
- Admin account passwords must be stored in a password manager

### 3.7 Temporary Contractor Access

- Temporary contractors (e.g., Cloud202 team) with admin-level access for specific project work:
  - Are documented in the Admin Account Register with start and end dates
  - Have their access reviewed monthly during the contract period
  - Have all access removed within 24 hours of contract end
  - Are subject to this policy during their engagement

## 4. COMPLIANCE

---

Violation of this policy may result in:

- Immediate revocation of admin access
- Disciplinary action
- Cyber Essentials certification failure

## 5. REVIEW SCHEDULE

---

This policy will be reviewed annually and updated as needed.

**APPROVED BY:**

Andrew James, CEO Halved Limited Date: 6th May 2026

Questions about data protection? [dataprivacy@halved.io](mailto:dataprivacy@halved.io)

Website [halved.io](https://halved.io) · students log in at [my.halved.io](https://my.halved.io)

Halved Limited · registered in England and Wales, company number 15261677 · last updated June 2026