Leamington Community Primary School

Together we make a Difference

Account Reconciliation Plan




Completed by: Mrs. A. Belger (Computing Subject Leader) and Matthew Kicks (Computeam)

Courage Determination Friendship Honesty Respect

Purpose of this plan:

To ensure that all user accounts, privileged accounts, service accounts and device accounts in the IT network are valid, correctly permissioned and free from discrepancies, thereby reducing security risk and maintaining compliance.

Scope:

- Active Directory / LDAP user accounts
- Local accounts on servers, workstations, network devices (switches, routers, firewalls)
- Privileged / administrative accounts
- Service / application accounts
- Temporary / guest / contractor accounts
- Group memberships, access permissions, and account metadata (last login, status)

Objectives & Metrics

Objective	Target / Goal	Metric(s)
Only valid accounts exist	Identify and disable or remove stale / unused accounts	Number / % of accounts inactive > 90 days
Permissions align with least privilege	Detect over-privileged accounts and remediate	Number of accounts with excessive rights
Service accounts are secure and managed	Ensure service credentials are rotated and stored securely	% of service accounts in vault, rotation frequency met
Regular reconciliation completed and documented	All scheduled reviews done on time	% of reconciliations completed vs planned

Roles & Responsibilities

Role	Responsibilities
IT Security Lead / Identity & Access Manager	Oversee reconciliation process, define policy, review results
System / AD Administrator	Extract account data, implement changes, coordinate with IT
Compliance / Audit	Review reconciliation logs, validate proper procedure
HR / Contractor Management	Notify IT of joiners / leavers / role changes to support reconciliation

Policies & Standards

- **Account Lifecycle Policy:** Define how accounts are created, modified, disabled, removed.
- **Least Privilege Principle:** Permissions should be minimal necessary for role.
- **Inactivity Policy:** Accounts inactive for a threshold (e.g. 90 days) are flagged, disabled, and later removed.
- **Password / Credential Policy:** Strong passwords, rotation, storage in vault, no shared credentials.
- **Privileged Account Handling:** Privileged accounts must be managed, monitored, and subject to stricter controls.
- **Access Review Frequency:** Regular (e.g. quarterly) reviews of accounts, permissions, groups.

Reconciliation Schedule & Frequency

Account Type / Area	Frequency	Deadline / Review Period
Privileged / service accounts	Monthly or bi-monthly	Within 5 business days after period end
User accounts (AD / LDAP)	Quarterly	Within 10 business days after quarter end
Local accounts (servers / devices)	Quarterly	Within 10 business days after quarter end
Temporary / guest / contractor accounts	Monthly	Within 5 business days after month end
Group membership / permissions review	Quarterly (or more frequent for sensitive groups)	Within 10 business days after period end
Role / HR changes (joiners / leavers)	On change	Within 24 hours of notification

Data Collection & Tools

- Export lists of accounts from directory (AD, LDAP), service accounts, local accounts.
- Extract group memberships, permissions, role assignments, last login timestamps.
- Access PAM / vault system data for service / privileged accounts.
- Use scripts / tools (PowerShell, identity management tools) to generate reports.
- For network devices, extract admin / local account lists via configuration / management interfaces.

Reconciliation Procedure & Workflow

Step	Key Activities
1. Data Extraction & Baseline Creation	Collect current account and permission data. Generate reports for inactive accounts and accounts with elevated permissions.
2. Exception Identification	Flag accounts with no login activity beyond threshold. Identify permissions beyond policy or orphaned service accounts.
3. Review & Triage	Categorise exceptions by risk level. Determine required action such as disable, delete, adjust, or rotate password.
4. Remediation & Execution	Disable or remove stale accounts. Adjust permissions or group membership. Rotate credentials for service accounts and document all changes.
5. Review & Approval	Reconciliation preparer reviews proposed changes. IT Security Lead or designated reviewer approves changes.
6. Validation & Testing	Test that changes did not negatively affect system access. Confirm staff and services retain required access.
7. Documentation / Audit Trail	Maintain logs of reports, exceptions, changes, and approvals including dates and responsible personnel for audit purposes.
8. Follow-Up	Track unresolved exceptions and reassess them in the next reconciliation cycle.

Controls & Monitoring

To maintain strong access governance and reduce the risk of privilege misuse, Leamington Community Primary School implements continuous monitoring and control measures for all privileged and administrative accounts. Automated alerts are configured to notify the IT Security Lead or system administrator whenever new privileged accounts are created, ensuring that no elevated access is granted without the proper authorisation. Account activity and login logs are regularly monitored to identify dormant or inactive accounts, allowing the school to promptly review, disable, or remove any that are no longer required. Periodic reviews of user permissions and group memberships are carried out to confirm that access rights remain consistent with the principle of least privilege and that staff have only the permissions necessary for their roles.

All changes to privileged or administrative accounts—including account creation, modification, or deletion—are logged in detail to provide a complete and auditable record for compliance and safeguarding purposes. These logs are reviewed regularly as part of the school's ongoing cyber security governance. Leamington Community Primary School enforces strict segregation of duties within this process: the review and approval of account changes are performed by individuals separate from those responsible for implementing them. This separation ensures oversight, prevents unauthorised actions, and upholds accountability across all IT and administrative systems. Collectively, these controls form part of the school's wider commitment to maintaining the security, integrity, and reliability of its digital infrastructure and the protection of pupil and staff data.

Reporting & Dashboards

Key metrics to report:

- Number of stale / inactive accounts disabled or removed
- Number of accounts with excessive privileges corrected
- Service account compliance (vault usage / rotation)
- Percentage of reconciliation completed on schedule
- Outstanding exceptions and aging

Reporting frequency: monthly or quarterly to management / security committee.

Format: summary dashboards + details of exceptions, actions taken, trends over time.

Risk & Mitigation

Risk	Impact	Mitigation
Inactive accounts not removed → security risk	Unauthorized or dormant account misuse	Use logs, last login checks, enforce inactivity policy
Incorrect removal / disabling → service disruption	Loss of legitimate access	Review before action, have rollback plans
Service accounts unmanaged → credential exposure	High risk of breach	Vault management, credential rotation, audit logs
Over-privileged accounts persist	Elevated risk	Least privilege, regular audits, corrections

Poor documentation → audit or compliance gaps	Incomplete evidence trail	Maintain logs, approvals, versioning

Reconciliation Checklist (Per Cycle)

- Export full account list (AD / LDAP / Directory)
- Export privileged / service / local accounts
- Retrieve last login / activity metrics
- Identify inactive / dormant accounts
- Identify over-privileged accounts
- Identify orphaned or unmanaged service accounts
- Review group membership vs role assignments
- Document all exceptions
- Propose remediation actions
- Obtain approval for changes
- Execute changes (disabling / deletion / adjustment / credential rotation)
- Test impacted systems / verify functionality
- Document changes, approvals, users impacted
- Update reconciliation master log / tracker
- Report to management / security team