Least Privilege Access SOP

Purpose

The purpose of this SOP is to enforce the principle of least privilege across all organizational systems and services. Access rights will be granted only to the minimum level necessary for staff to perform their duties, reducing the risk of unauthorized actions, accidental changes, or security breaches.

1. Roles and Permissions

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Role** | **Google** | **Microsoft** | **Synology 1** | **Synology 2** | **Ubiquiti** |
| Executive Director | Super admin | Super admin | Super admin | Super admin | Super admin |
| Human Resources | Super admin | Super admin | Super admin | Super admin | Super admin |
| IT Lead | Super admin | Admin (most settings) | Super admin | Super admin | Super admin |
| IT Team | Admin (specific settings) | Admin (specific settings) | Admin (specific settings) | Admin (specific settings) | Admin (specific settings) |
| Directors | Timed admin or Viewer (by request) | Timed admin or Viewer (by request) | Time admin or Viewer (by request) | Timed admin or Viewer (by request) | Admin (Director of Operations only); Timed admin or Viewer (others by request) |
| Supervisors | Viewer (by request) | Viewer (by request) | Viewer (by request) | Viewer (by request) | Viewer (by request) |
| Media Lead | No access | No access | No access | Admin | No access |
| Operations Department Staff | No access | No access | No access | No access | Viewer (by Director of Operations approval) |

NOTES:

* Super admin = unrestricted access to all system settings
* Admin = access to most configuration settings, if not all, but not super admin controls
* Timed admin = temporary admin rights granted for a defined period (requires approval)
* Viewer = read-only access

1. Policy
2. Default access: All staff are provisioned with the minimum access necessary for their job role.
3. Super admin restrictions: Only Executive Director and Human Resources hold super admin rights for all services. IT Lead holder super admin for Google, Synology, and Ubiquiti, and admin rights for Microsoft.
4. Timed admin rights: Granted to Directors only upon documented request, for a defined period, and revoked immediately after the approved task is complete.
5. Viewer access by request: Directors and Supervisors may request viewer access to any system when business needs justify it; Operations staff may request viewer access to Ubiquiti via Director of Operations.
6. Access change documentation: All role changes must be logged with request date, approver, start date, and end date.
7. Quarterly review: IT will conduct quarterly reviews of access privileges to ensure compliance with this policy.
8. Procedure
9. Upon receipt of role change request, verify request against the above policy, confirm role eligibility, and log the request.
10. Apply access change in the respective system’s admin portal.
11. Confirm access with requestor.
12. Update log with date and time of change.
13. Revoke timed admin access when needed.
    1. Review the log for upcoming expiry dates.
    2. Remove elevated privileges in the admin portal.
    3. Document revocation date and time in the log.
    4. Notify the requester that admin rights have been revoked.
14. Audit user roles for all systems quarterly.
    1. Export user role reports from all systems.
    2. Compare roles against the approved matrix above.
    3. Remove or downgrade any roles that exceed approved privileges.
    4. Document review findings and corrective actions.
15. Report any deviation from this procedure and policy that is without documented approval to the Executive Director and HR.

This SOP must be reviewed annually or upon changes in systems or organizational restructuring.