# Expanded User Access Review (UAR) Documentation

## Purpose

Objective: To rigorously monitor and verify that all access rights within the organization are granted appropriately and remain aligned with users' current job responsibilities, minimizing the risk of internal and external security breaches.

## Scope

Applicability: Includes every digital and physical access point within the organization, from enterprise systems to office security systems. Applies to all full-time, part-time employees, contractors, and third-party service providers.

## Policy Overview

Review Frequency: Reviews should occur semi-annually, with additional ad-hoc reviews triggered by major system changes, significant job role updates, or security incidents.

## Procedures

Planning and Preparation: Collect roles from HR, inventory access rights, establish review schedule.  
Conducting Reviews: Use automated tools for scanning, conduct manual checks and stakeholder interviews.  
Reporting Findings: Generate comprehensive reports, hold review meetings with stakeholders.  
Remediation Actions: Revoke unauthorized access immediately, update access control processes.

## Roles and Responsibilities

UAR Coordinator: Manages the UAR process, ensures timely execution.  
System Owners: Provide access logs, validate access rights.  
Security Analysts: Analyze access logs, report anomalies.

## Compliance and Regulations

Regulatory Mapping: Detail compliance with GDPR, HIPAA, SOX. Maintain logs of all UAR activities for audits.

## Tools and Technologies

IAM Systems: Use SailPoint, Okta, or Microsoft Azure AD for automating UAR process. Use analytics tools to detect access anomalies.

## Training and Awareness

Regular Workshops: Organize quarterly workshops on security hygiene and the UAR role. Conduct post-review feedback sessions.

## Evaluation and Improvement

KPIs: Define performance indicators such as discrepancies per review, resolution time, user satisfaction. Establish feedback loop for process improvement.

## Annexes

Detailed Checklists: Provide checklists for each access review type. Include sample forms for reporting discrepancies, requesting changes, confirming review completion.