Access Review Procedures

Document ID: IT-SEC-025 **Last Updated:** March 2024 **Owner:** IT Security
Applies To: All Systems and Applications

Purpose

Regular access reviews ensure that user access rights remain appropriate, comply with the principle of least privilege, and meet regulatory requirements (SOC 2, ISO 27001, HIPAA, PCI-DSS).

Review Schedule

Frequency by System Type

System Type	Review Frequency	Owner
Production infrastructure	Monthly	SRE Team
Customer data systems	Monthly	Data Team
Financial systems	Quarterly	Finance
HR systems	Quarterly	HR
Development systems	Quarterly	Engineering
General IT systems	Semi-annually	IT
SaaS applications	Semi-annually	IT

Frequency by Access Level

Access Level	Review Frequency
Admin/Privileged	Monthly
Write access to sensitive data	Monthly
Standard user access	Quarterly
Read-only access	Semi-annually

Review Process

Step 1: Generate Access Report

IT Security generates reports showing: - All users with access - Access level/permissions - Last access date - Department and manager - Account creation date

Tools: - Okta: User provisioning reports - AWS: IAM Access Analyzer - GitHub: Organization access report - Custom scripts for internal systems

Step 2: Distribute for Review

Reports distributed to reviewers: - System owners - Department managers - Data owners

Timeline: Reviews due within 10 business days

Step 3: Manager Review

Managers review their team members' access:

Question	Action if No
Is this person still on my team?	Remove access
Do they need this access level?	Reduce access
Have they used access in 90 days?	Consider removal
Is access appropriate for their role?	Adjust access

Step 4: Document Decisions

For each user, managers document: - **Approve:** Access confirmed appropriate - **Modify:** Access level changed - **Remove:** Access revoked - **Justification:** Reason for decision

Step 5: Implement Changes

IT implements access changes: - Same day for removals - Within 3 business days for modifications - Notify affected users

Step 6: Audit Trail

All reviews documented: - Review date - Reviewer - Decisions made - Changes implemented - Exceptions approved

---

Systems Requiring Review

Tier 1: Critical (Monthly)

System	Owner	Reviewer
AWS Production	SRE	VP Engineering
Customer Database	Data Team	Data Lead
SecureVault	Security	CISO
Payment Systems	Finance	CFO
Kubernetes Clusters	Platform	Platform Lead

Tier 2: Sensitive (Quarterly)

System	Owner	Reviewer
GitHub (org admin)	Engineering	VP Engineering
Salesforce	Sales Ops	VP Sales
Workday	HR	CPO
NetSuite	Finance	CFO
DataLens (admin)	Data Team	Data Lead

Tier 3: Standard (Semi-annually)

System	Owner	Reviewer
Google Workspace	IT	IT Director
Slack	IT	IT Director
Confluence	IT	Department Heads
Zoom	IT	IT Director
Jira	Engineering	Engineering Managers

Privileged Access Reviews

Monthly Requirements

All privileged access reviewed monthly:

1. **Admin accounts**
   - Root/superuser access
   - Domain admin
   - AWS Organizations admin
2. **Elevated permissions**
   - Production database write
   - Kubernetes cluster admin
   - Secret management admin
3. **Break-glass accounts**
   - Emergency access accounts
   - Verify unused
   - Rotate credentials if used

Privileged Access Checklist

☐ Account still needed?
☐ Minimum necessary permissions?
☐ MFA enabled?
☐ Activity logged?
☐ Used in past 30 days?
☐ Password/key rotated on schedule?

Terminated Employee Review

Immediate (Within 24 hours of termination)

☐ Disable Okta account
☐ Revoke VPN access
☐ Disable email
☐ Revoke GitHub access
☐ Remove from Slack

Within 7 days

- ☐ Review all system access
- ☐ Collect equipment
- ☐ Archive email/files
- ☐ Update shared credentials
- ☐ Document in HR system

Exceptions

Exception Process

1. Reviewer identifies need for exception
2. Document business justification
3. Risk assessment by Security
4. Approval by system owner + Security
5. Time-limited (max 90 days)
6. Logged in exception register

Exception Register

Field	Description
User	User requiring exception
System	System with exception
Access	Access being granted
Justification	Business reason
Risk	Risk assessment
Approver	Who approved
Expiration	When exception ends
Review date	Next review date

Reporting

Monthly Reports

IT Security produces: - Access review completion status - Changes made summary - Exceptions granted - Overdue reviews

Quarterly Reports

- Access trend analysis
- Compliance status
- Audit findings addressed
- Recommendations

Annual Reports

- Full access review summary
- Policy effectiveness
- Improvement recommendations
- Audit readiness assessment

Compliance Requirements

SOC 2

- User access reviews documented
- Privileged access reviewed quarterly (we do monthly)
- Terminated user access removed timely
- Evidence retained

ISO 27001

- Access rights reviewed regularly
- Privileged access controlled
- User registration and de-registration process
- Access control policy enforced

HIPAA (where applicable)

- PHI access reviewed
- Minimum necessary enforced
- Access logs reviewed

PCI-DSS (where applicable)

- Cardholder data access reviewed
- User IDs assigned individually

- Access removed when no longer needed

Automation

Automated Processes

Process	Automation Level	Tool
Report generation	Fully automated	Custom scripts
Report distribution	Fully automated	Email workflow
Review reminders	Fully automated	Slack bot
Access removal	Semi-automated	Okta workflows
Compliance reporting	Partially automated	Drata

Planned Automation

- Auto-expire unused access (90+ days)
- Risk-based review frequency
- ML-based anomaly detection

Roles and Responsibilities

IT Security

- Generate access reports
- Distribute for review
- Track completion
- Implement changes
- Maintain audit trail
- Report to compliance

System Owners

- Define appropriate access levels
- Approve/deny access requests
- Review privileged access monthly
- Escalate concerns

Managers

- Review team member access
- Document decisions
- Complete reviews on time
- Request new access as needed

Employees

- Request only necessary access
- Report unused access
- Use access appropriately
- Complete security training

Contact

- **IT Security:** security@novatech.com
- **Access Requests:** IT Service Portal
- **Urgent Matters:** security-urgent@novatech.com

Related Documents: Access Control Policy (IT-SEC-020), Privileged Access Management (IT-SEC-026), User Provisioning (IT-SEC-030)