Insider Threat

Investigation Playbook

Confidential Investigation Procedures

■ HIGHLY CONFIDENTIAL - RESTRICTED DISTRIBUTION ■

Version:	1.5
Last Updated:	February 2026
Classification:	HIGHLY CONFIDENTIAL
Document Owner:	Security Operations / Legal
Authorized Distribution:	SOC Lead, Legal, HR Director, CISO

Legal & Compliance Notice

CRITICAL LEGAL REQUIREMENTS:

• **Legal Counsel Involvement:** Consult with Legal department BEFORE initiating any investigation. Investigations may trigger employment law, privacy law, and evidence preservation requirements.

• **Privacy Compliance:** All investigations must comply with applicable privacy laws (GDPR, CCPA, etc.). Personal data collection must be proportionate and legally justified.

• **Evidence Preservation:** All evidence must be handled using forensically sound methods. Chain of custody must be maintained for potential legal proceedings.

• **HR Partnership:** Human Resources must be involved from the initial stages to ensure compliance with employment laws and company policies.

• **Confidentiality:** Investigation details must be shared on a strict need-to-know basis. Unauthorized disclosure may compromise the investigation and expose the company to liability.

• **Anti-Retaliation:** Whistleblowers and witnesses must be protected from retaliation. Document all protections provided.

Table of Contents

1. Investigation Framework & Governance

1.1 Investigation Triggers

An insider threat investigation may be initiated based on the following triggers:

Trigger Source	Examples	Severity
Automated Alerts	DLP violations, abnormal access patterns, privilege escalation	Medium-High
Manager Report	Behavioral changes, policy violations, suspicious activities	Medium
Employee Report	Whistleblower complaints, observed violations	Medium-High
HR Notification	Performance issues, disciplinary history, resignation notice	Low-Medium
Third-Party Report	Vendor notifications, law enforcement contact	High
Audit Findings	Access anomalies, compliance violations	Medium

1.2 Investigation Team Structure

Role	Responsibilities	Required For
Investigation Lead	Case management, evidence coordination, reporting	All cases
Legal Counsel	Legal guidance, privilege review, litigation prep	All cases
HR Partner	Employment law compliance, policy interpretation	All cases
SOC Analyst	Log analysis, SIEM queries, technical investigation	Technical cases
Forensics Specialist	Evidence collection, disk imaging, forensic analysis	High severity
IT Security Engineer	Access review, system analysis, containment	All cases
Manager/Supervisor	Context, behavioral observations, business impact	As needed

1.3 Severity Classification

Level	Criteria	Response Time	Escalation
Critical	Active data exfiltration Sabotage in progress Imminent harm	Immediate	CISO, Legal, HR Director
High	Large-scale data access Privilege abuse Post-resignation activity	4 hours	Security Manager, Legal, HR
Medium	Policy violations Abnormal access patterns Minor data exposure	24 hours	SOC Lead, HR Partner

Low	Potential indicators Requires validation Monitoring only	72 hours	SOC Analyst

2. Behavioral Indicators of Insider Threats

2.1 Threat Categories & Motivations

Understanding threat actor profiles helps identify indicators and predict behavior:

Profile	Motivation	Common Indicators	Risk Level
Malicious Insider	Financial gain Revenge Ideology	Data exfiltration Deliberate policy violations Covert behavior	High
Negligent Employee	Carelessness Lack of awareness	Repeated violations Ignoring warnings Poor security hygiene	Medium
Compromised Account	External actor using credentials	Abnormal hours New locations Unusual activities	High
Departing Employee	Taking data to new job Competitive advantage	Massive downloads Access to non-job files USB usage	High

2.2 Observable Behavioral Indicators

These behavioral changes may indicate elevated insider threat risk:

Professional Behavior Changes:

• Sudden performance decline or disengagement from work

• Increased conflicts with management or colleagues

• Violation of company policies (especially security-related)

• Resistance to supervision or refusal to follow procedures

• Unusual interest in matters outside job scope

• Questions about security controls or monitoring systems

• Attempts to access information beyond job requirements

Personal Circumstance Indicators:

• Expressed job dissatisfaction or intent to leave

• Financial difficulties or sudden lifestyle changes

• Recent disciplinary action or negative performance review

• Known contact with competitors or recruitment activities

• Personal crisis (divorce, health issues, substance abuse)

• Ideological grievances or extremist views

- Acceptance of job offer with competitor (resignation submitted)

Work Pattern Changes:

- Working unusual hours (late night, weekends) without business justification
- Coming in outside normal schedule when office is empty
- Increased remote work or VPN usage
- Taking work materials home without authorization
- Reluctance to take vacation or complete knowledge transfer
- Installing unauthorized software or hardware
- Photographing screens or documents

2.3 Risk Scoring Matrix

Use this matrix to quantify risk levels based on multiple indicators:

Indicator Category	Low Risk (1pt)	Medium Risk (2pts)	High Risk (3pts)
Behavioral Changes	Minor/isolated	Multiple indicators	Severe/persistent
Access Patterns	Normal variation	Some anomalies	Significant deviation
Data Handling	Within scope	Occasional excess	Systematic exfiltration
Policy Compliance	Minor violations	Repeated violations	Deliberate circumvention
Employment Status	Stable	Performance issues	Departure pending

Risk Score Interpretation: 5-7 points = Low Risk (monitor), 8-11 points = Medium Risk (investigate), 12-15 points = High Risk (immediate action)

3. Initial Assessment & Case Initiation

3.1 Initial Triage Process

Receive Alert/Report (T+0): Document source, time, and initial details. Assign case number and Investigation Lead.

Preliminary Review (T+1 hour): Review available data without alerting subject. Determine if investigation is warranted.

Legal Consultation (T+2 hours): Brief Legal counsel on facts. Obtain guidance on investigation scope and methods.

HR Notification (T+4 hours): Notify HR partner. Review employment file, disciplinary history, and any active HR matters.

Severity Assessment (T+4 hours): Classify case severity. Determine investigation team composition.

Investigation Plan (T+8 hours): Document investigation objectives, scope, timeline, and resource needs.

Kickoff Meeting (T+24 hours): Brief investigation team. Assign tasks and establish communication protocols.

3.2 Investigation Planning Template

- **Case Information:** Case ID, Subject Name/Employee ID, Date Opened, Assigned Lead
- **Allegation Summary:** Brief description of suspected violation or concerning behavior
- **Investigation Scope:** Systems to review, time period, data types, geographic scope
- **Legal Considerations:** Applicable laws, privilege issues, union considerations
- **Investigation Team:** Roles assigned with contact information
- **Evidence Sources:** SIEM logs, AD logs, DLP alerts, email, file systems, endpoints
- **Containment Measures:** Access restrictions, monitoring enhancements (if applicable)
- **Timeline:** Key milestones with target dates
- **Success Criteria:** What findings would confirm/refute the allegation
- **Communication Plan:** Stakeholder updates, frequency, confidentiality requirements

3.3 Covert vs. Overt Investigation Decision

Factor	Covert Investigation	Overt Investigation
Subject Awareness	Subject unaware	Subject notified of investigation
When to Use	Active threat Evidence gathering Flight risk	Policy violation Negligence Low flight risk

Advantages	Preserves evidence Prevents destruction Observes ongoing activity	Legal transparency Reduces liability Easier to justify
Risks	Privacy concerns Potential legal challenges	Evidence destruction Continued malicious activity
Legal Requirement	Legal approval required	Standard HR notification

CRITICAL: Covert investigations require Legal approval and must be justified by legitimate business need and proportionate to the risk.

4. SIEM Alert Patterns & Detection (Splunk)

4.1 High-Risk Activity Searches

Execute these Splunk searches to identify potential insider threat indicators:

Massive File Downloads:

```
index=file_access action=download user=[username]
| stats sum(file_size) as total_mb, count as download_count by user, src_ip
| eval total_gb=round(total_mb/1024,2)
| where total_gb > 10 OR download_count > 1000
| sort -total_gb
```

After-Hours Access Anomalies:

```
index=authentication user=[username] action=success
| eval hour=strftime(_time,"%H")
| where (hour<6 OR hour>22)
| stats count by user, src_ip, hour
| sort -count
```

Unauthorized Access Attempts:

```
index=windows EventCode=4663 user=[username]
| eval accessed_file=Object_Name
| search accessed_file="*confidential*" OR accessed_file="*executive*" OR accessed_file="*HR*"
| stats count by user, accessed_file, src_computer
| where count > 5
```

USB/Removable Media Usage:

```
index=endpoint EventCode=2003 OR EventCode=2100 user=[username]
| eval device_type=case(like(Device_Description,"%USB%"),"USB Storage",
like(Device_Description,"%External%"),"External Drive", 1=1,"Other")
| stats count, values(Device_Description) as devices by user, device_type
| sort -count
```

Cloud Upload Activities:

```
index=proxy user=[username] (url="*dropbox.com*" OR url="*drive.google.com*" OR url="*onedrive*"
OR url="*box.com*")
| stats sum(bytes_out) as uploaded_bytes, count by user, url, src_ip
| eval uploaded_mb=round(uploaded_bytes/1048576,2)
| where uploaded_mb > 100
| sort -uploaded_mb
```

Privilege Escalation Attempts:

```
index=windows (EventCode=4672 OR EventCode=4673) user=[username]
| stats count by user, Privileges, Computer_Name
| where count > 10
| sort -count
```

4.2 Data Exfiltration Detection

Email Exfiltration Pattern:

```
index=email sender=[username]
| eval is_external=if(like(recipient,"%@company.com"),"Internal","External")
| search is_external="External"
| stats sum(attachment_size) as total_mb, count as email_count, values(recipient) as recipients by
sender
| eval total_gb=round(total_mb/1024,2)
| where total_gb > 1 OR email_count > 50
| sort -total_gb
```

Sensitive File Access:

```
index=dlp user=[username] action=violation
| stats count by user, policy_violated, file_name, destination
| sort -count
```

Database Query Anomalies:

```
index=database user=[username] query_type=SELECT
| eval rows_returned_k=round(rows_returned/1000,1)
| where rows_returned_k > 100
| stats count, avg(rows_returned_k) as avg_rows, max(rows_returned_k) as max_rows by user,
database_name
| sort -max_rows
```

4.3 Account Compromise Indicators

Impossible Travel Detection:

```
index=authentication user=[username] action=success
| iplocation src_ip
| streamstats current=f last(_time) as last_time, last(City) as last_city by user
| eval time_diff_hours=round((_time-last_time)/3600,2)
| where City!=last_city AND time_diff_hours<4
| table _time, user, City, last_city, time_diff_hours, src_ip
```

Multiple Failed Logins Followed by Success:

```
index=authentication user=[username]
| transaction user maxspan=5m
| search action=failed action=success
| stats count by user, src_ip, _time
| sort -count
```

4.4 Investigation Dashboard Creation

Create a dedicated Splunk dashboard for the subject under investigation. Include these panels:

- Authentication timeline with source IPs and locations
- File access volume (downloads, deletions, modifications)
- Email activity (internal vs external, attachment sizes)
- Cloud storage uploads/downloads
- Removable media events (USB, external drives)
- Application usage patterns
- Network connections (especially non-standard ports)
- DLP policy violations
- Privilege changes or sudo/admin command usage
- After-hours activity heatmap

4.5 Alert Correlation & Risk Scoring

Use this query to create a comprehensive risk score based on multiple indicators:

```
| multisearch
[search index=file_access user=[username] action=download | stats count as file_downloads ]
[search index=email sender=[username] recipient!=*@company.com | stats count as ext_emails ]
[search index=authentication user=[username] hour<6 OR hour>22 | stats count as after_hours ]
[search index=dlp user=[username] | stats count as dlp_violations ]
[search index=endpoint user=[username] EventCode=2003 | stats count as usb_events ]
| eval
risk_score=(file_downloads*2)+(ext_emails*3)+(after_hours*1)+(dlp_violations*5)+(usb_events*4)
| eval risk_level=case(risk_score>100,"Critical", risk_score>50,"High", risk_score>20,"Medium",
1=1,"Low")
```

5. Active Directory Access Review

5.1 User Account Analysis

Review the subject's Active Directory account for indicators of malicious activity:

PowerShell: Get User Account Details

```
Get-ADUser -Identity [username] -Properties * | Select-Object
Name, SamAccountName, EmailAddress, Department, Title, Manager,
Created, Modified, LastLogonDate, PasswordLastSet, PasswordNeverExpires,
Enabled, LockedOut, AccountExpirationDate, MemberOf,
whenChanged, DistinguishedName
```

Review Group Memberships:

```
Get-ADPrincipalGroupMembership -Identity [username] |
Select-Object Name, GroupCategory, GroupScope |
Sort-Object Name | Format-Table -AutoSize
```

Key Items to Document:

- All group memberships (especially privileged groups: Domain Admins, Enterprise Admins, etc.)
- Recent group membership changes (additions/removals in last 90 days)
- Delegated permissions or custom ACLs
- Service accounts or application access
- Recent password changes (especially just before/after suspicious activity)
- Account lockouts or failed login attempts
- Changes to account attributes (email, phone, manager)
- Multiple accounts for same user (check for privilege separation violations)

5.2 Access Rights Audit

File Share Permissions:

```
# Get all file shares the user can access
Get-SmbShare | ForEach-Object {
$shareName = $_.Name
$sharePath = $_.Path
Get-SmbShareAccess -Name $shareName | Where-Object {
$_.AccountName -like "*[username]*"
} | Select-Object @{N="Share";E={$shareName}}, AccountName, AccessRight
}
```

Identify Sensitive Data Access:

```
# Search for user access to files/folders containing sensitive keywords
Get-ChildItem -Path "\\fileserver\shares" -Recurse |
Where-Object {$_.Name -match "confidential|executive|financials|HR"} |
Get-Acl | Where-Object {
$_.Access | Where-Object {$_.IdentityReference -like "*[username]*"}
} | Select-Object Path, Owner, @{N="User";E={$_.Access.IdentityReference}}
```

5.3 Authentication & Access Logs

Windows Event Log Review:

Event ID	Description	Investigation Value
4624	Successful logon	Login times, source IPs, logon type
4625	Failed logon	Brute force attempts, account probing
4648	Logon with explicit credentials	RunAs or credential theft
4672	Special privileges assigned	Admin privilege usage
4768/4769	Kerberos TGT/Service ticket	Service access, lateral movement
4663	Object access attempt	File/folder access attempts
5140	Network share access	File share connections
4720	User account created	Unauthorized account creation
4728/4732	Member added to group	Privilege escalation

PowerShell: Extract Authentication Events

```
Get-WinEvent -FilterHashtable @{
LogName="Security"
ID=4624,4625,4648,4672
} | Where-Object {$_.Message -like "*[username]*"} |
Select-Object TimeCreated, ID, Message |
Export-Csv -Path "auth_events_[username].csv" -NoTypeInformation
```

5.4 Privileged Access Review

If the subject has or had privileged access, conduct enhanced review:

- **Administrative Activity:** Review all actions taken with elevated privileges (domain admin, local admin, application admin)
- **Service Account Access:** Check if user has access to service account credentials or can reset service account passwords
- **Delegation Rights:** Identify any delegated permissions that could be abused (password reset, group management, GPO editing)
- **Recent Privilege Changes:** Document when privileges were granted/revoked and by whom
- **PAM/JIT Access:** Review Privileged Access Management logs for just-in-time elevation requests and usage

- **Shadow Admin Detection:** Look for non-obvious privilege paths (nested groups, ACL-based permissions, local admin on critical servers)

6. Digital Evidence Collection

CRITICAL LEGAL REQUIREMENT: All evidence collection must be performed using forensically sound methods to ensure admissibility in legal proceedings. Consult Legal before collecting evidence.

6.1 Evidence Types & Collection Methods

Evidence Type	Collection Method	Tools	Legal Considerations
Log Data	SIEM export Direct log collection	Splunk Elasticsearch Windows Event Viewer	Ensure logs not altered Maintain timestamps
Email	Legal hold Mailbox export	eDiscovery tools PowerShell (Exchange)	Privacy laws Attorney-client privilege
Files	Forensic copy Hash verification	FTK Imager EnCase dd/dcfldd	Chain of custody Integrity verification
Endpoint	Disk image Memory dump	FTK Imager Magnet RAM Capture WinPMEM	Minimize system changes Document collection
Network	PCAP files Flow records	Wireshark NetFlow Zeek	PII redaction Retention limits
Database	Query results Audit logs	Native DB tools Splunk DB Connect	Data minimization Access authorization
Mobile/BYOD	MDM logs App data export	MDM console Mobile forensics tools	Personal data separation Consent required

6.2 Chain of Custody Requirements

Maintain detailed chain of custody documentation for all evidence:

- **Initial Collection:** Who collected, what was collected, when, where, how (method/tools)
- **Hash Values:** MD5, SHA-1, and SHA-256 hashes for all files and disk images
- **Storage Location:** Physical location, access controls, encryption status
- **Access Log:** Everyone who accessed evidence, purpose, date/time
- **Transfer Log:** Any movement of evidence between people/systems
- **Disposal:** When and how evidence was destroyed (if applicable)
- **Continuity:** Ensure no gaps in custody documentation

6.3 Endpoint Forensics Collection

Live System Triage (Volatile Data):

Collect volatile data before powering down or imaging:

```
# Memory dump (Windows)
winpmem_mini_x64.exe -o memory.raw

# Running processes
Get-Process | Export-Csv processes.csv

# Network connections
netstat -ano > network_connections.txt

# Logged-in users
query user > logged_users.txt

# Loaded DLLs
Get-Process | Select-Object Name, Modules | Export-Csv loaded_dlls.csv
```

Disk Imaging (Non-Volatile Data):

Create forensic image of the system drive:

```
# Using FTK Imager (GUI) or command line:
ftkimager.exe [PhysicalDrive] [output_path] --e01 --compress 6 --verify

# Or using dd (Linux/Mac):
sudo dd if=/dev/sda of=/mnt/evidence/disk_image.dd bs=4M status=progress
sha256sum /mnt/evidence/disk_image.dd > /mnt/evidence/disk_image.sha256
```

6.4 Email & Communication Evidence

Exchange/Office 365 Mailbox Export:

```
# Place mailbox on litigation hold first
Set-Mailbox -Identity [username] -LitigationHoldEnabled $true

# Export mailbox to PST
New-MailboxExportRequest -Mailbox [username] -FilePath "\\fileserver\exports\[username].pst"

# Check export status
Get-MailboxExportRequest | Get-MailboxExportRequestStatistics
```

Search for Specific Content:

```
# Search for emails with attachments to external recipients
Search-Mailbox -Identity [username] -SearchQuery "hasattachment:true AND to:*@competitor.com"
-TargetMailbox "eDiscovery" -TargetFolder "Investigation_[CaseID]"
```

6.5 Cloud & SaaS Evidence

For cloud services, collect evidence via native audit logs and APIs:

- **Office 365 Audit Logs:** Use Microsoft Purview Compliance portal or PowerShell to export unified audit logs
- **Google Workspace:** Admin console > Reporting > Audit and investigation > Export
- **Salesforce:** Setup > Security > View Setup Audit Trail, Export event logs via API
- **AWS:** CloudTrail logs, CloudWatch logs, S3 access logs via AWS CLI or Console
- **Box/Dropbox:** Admin console activity logs, use eDiscovery features if available
- **Slack/Teams:** Export workspace data, review DM logs (requires legal process)

Important: Cloud data may have retention limits (30-90 days). Initiate legal hold and export evidence early in investigation.

7. HR Coordination Procedures

7.1 HR Partnership Requirements

Human Resources must be involved from investigation initiation through resolution:

Investigation Stage	HR Responsibilities	Required Documentation
Initiation	• Review employment file • Check disciplinary history • Identify union/contract issues • Assess termination risk	Employee file Performance reviews Prior incidents
Planning	• Advise on employment laws • Review investigation scope • Coordinate with Legal • Plan for contingencies	Investigation plan Legal consultation notes
Active Investigation	• Monitor subject behavior • Coordinate manager communication • Document HR-related findings • Prepare for interviews	Behavioral observations Manager reports Policy violations
Interview	• Attend investigative interviews • Ensure policy compliance • Document statements • Assess credibility	Interview transcripts Witness statements
Resolution	• Recommend employment action • Draft termination letter • Coordinate final paycheck • Exit interview (if applicable)	Disciplinary action form Termination checklist
Post-Investigation	• Process references • Handle unemployment claims • Document lessons learned • Update policies if needed	Case closure report Policy updates

7.2 Employment File Review

HR should provide comprehensive employment history for context:

- Employment start date, position history, promotions/demotions
- Current job description and access requirements
- Performance reviews (last 3 years minimum)
- Disciplinary history (verbal warnings, written warnings, PIPs)
- Prior security incidents or policy violations
- Grievances filed or complaints made
- Salary, bonuses, stock options (financial motivation context)
- Benefits status (medical, retirement contributions)
- Manager change history

- Transfer requests or internal applications
- Training records (security awareness, code of conduct)
- Signed acknowledgments (AUP, confidentiality agreements, non-compete)

7.3 Manager Coordination

The subject's direct manager plays a critical role. HR coordinates manager involvement:

- **Confidentiality Briefing:** Manager must understand investigation is confidential. No disclosure to subject or other employees.
- **Behavioral Observations:** Manager documents any changes in work habits, attitude, performance, or interpersonal relationships.
- **Work Product Review:** Manager may be asked to review quality of work, attendance patterns, deadline compliance.
- **Operational Context:** Manager explains business justification (or lack thereof) for subject's data access or activities.
- **Communication Management:** HR and Legal approve all manager communications with subject during investigation.
- **No Retaliation:** Manager must treat subject normally unless directed otherwise. Document any subject concerns about treatment.
- **Exit Planning:** If termination likely, manager prepares for knowledge transfer, project reassignment, team notification.

7.4 Workplace Accommodations During Investigation

Scenario	HR Action	Justification Required
Access Restriction	Disable VPN, revoke sensitive system access	Yes - business need, not punitive
Administrative Leave	Paid leave pending investigation completion	Yes - Legal/HR approval, severity-based
Work Location Change	Remote work or office relocation	Yes - investigative necessity
Monitoring Enhancement	Increase logging, DLP sensitivity	Yes - proportionate to risk
Manager Reassignment	Report to different manager temporarily	Yes - avoid bias or retaliation
Project Removal	Reassign from sensitive projects/clients	Yes - business justification

CAUTION: Any action that alters the subject's employment status or conditions must be defensible as necessary for investigation or business operations. Avoid actions that could be perceived as pre-judging guilt or retaliation.

7.5 Employment Action Decision Matrix

Finding	Severity	Typical HR Action	Legal Considerations

Unsubstantiated	N/A	Close case No action Restore access if restricted	Document thoroughly Protect from retaliation Consider false accuser
Policy violation (minor)	Low	Verbal/written warning Retraining Monitoring period	Document in personnel file Ensure consistency with policy
Policy violation (major)	Medium	Final written warning PIP Privilege revocation	May require union notification Document improvement plan
Data mishandling (negligence)	Medium-High	Suspension Retraining Role change May terminate	DLP policy enforcement Data breach notification requirements
Intentional data theft	High	Immediate termination Law enforcement referral Civil action	Preserve evidence Non-compete enforcement Trade secret protection
Sabotage/destruction	Critical	Immediate termination Criminal referral Injunction	Emergency access revocation Incident response Insurance notification

8. Interview & Documentation

8.1 Interview Planning & Preparation

- **Interview Objectives:** Define what you need to learn. Prepare specific questions but remain flexible to follow investigative leads.
- **Interview Team:** Minimum 2 people (Investigation Lead + HR or Legal). One asks questions, one takes detailed notes.
- **Location:** Private, neutral conference room. Ensure no interruptions. Consider recording (with consent and Legal approval).
- **Timing:** Early in work shift when subject is fresh. Allow adequate time (1-2 hours). Avoid Friday afternoons or before holidays.
- **Subject Rights:** Review applicable employee rights (union representation, legal counsel). Some jurisdictions require advance notice.
- **Evidence Review:** Interview team reviews all evidence beforehand. Know what you can disclose and what must remain confidential.
- **Documentation Ready:** Prepare witness statement form, acknowledge receipt forms, policy documents to reference.

8.2 Interview Structure & Best Practices

Phase	Duration	Objectives	Techniques
Introduction	5-10 min	Establish rapport Explain process Confirm rights	Professional but warm Clear explanation Document consent
Background	10-15 min	Get subject comfortable Establish baseline Understand role/access	Open-ended questions Active listening Build timeline
Core Questions	30-45 min	Address allegations Gather subject account Identify inconsistencies	Specific questions Silent pauses Follow-up probes
Evidence Presentation	10-20 min	Show relevant evidence Gauge reactions Allow explanations	Strategic disclosure Observe demeanor Document responses
Closing	5-10 min	Final questions Get commitment Explain next steps	Summarize key points Opportunity to add info Set expectations

8.3 Interview Red Flags & Deception Indicators

While not conclusive, these behaviors may indicate deception or evasion:

- Inconsistent timeline or contradictory statements
- Excessive detail about irrelevant matters, vague about key issues

- Repeated memory failures about critical events
- Deflection or blaming others without evidence
- Hostile or defensive reactions to straightforward questions
- Coaching questions ('What should I have done?')
- Invoking fifth amendment or refusing to answer specific questions
- Significant behavioral changes (calm to agitated or vice versa)

Note: Nervousness is normal in interviews. Do not assume guilt based on demeanor alone. Focus on factual inconsistencies and evidence contradictions.

8.4 Documentation Requirements

- **Interview Notes:** Detailed, contemporaneous notes. Quote significant statements verbatim. Note any pauses, emotional reactions, or behavioral changes.
- **Statement Form:** Have subject review and sign written summary of key points. Subject can add corrections or clarifications.
- **Acknowledgments:** Subject signs acknowledgment of company policies, data handling requirements, confidentiality obligations.
- **Evidence Receipt:** If subject surrenders devices, documents, or access credentials, document with receipt form.
- **Witness Statements:** Interview any witnesses separately. Document their observations, timeline, and any corroborating evidence.
- **Timeline Reconstruction:** Build detailed timeline of events using evidence and statements. Identify gaps and inconsistencies.
- **Evidence Matrix:** Create table linking allegations to evidence and subject responses.

9. Case Resolution & Remediation

9.1 Investigation Conclusion Process

Evidence Analysis Complete: All planned evidence collection and interviews completed. No new investigative leads.

Findings Documentation: Prepare comprehensive investigation report with timeline, evidence summary, and conclusions.

Legal Review: Legal counsel reviews findings and recommended actions. Assess litigation risk, employment law compliance.

HR Recommendation: HR proposes employment action based on findings and precedent. Consider progressive discipline policy.

Management Decision: Senior management (CISO, HR Director, Legal) make final decision on employment action and other remediation.

Implementation: Execute approved actions (termination, discipline, monitoring, training). Coordinate access revocation, equipment return.

Notification: Subject notified of findings and action. If termination, conduct exit meeting with HR and Security present.

Case Closure: Document final disposition, lessons learned, security improvements needed.

9.2 Termination Procedures (If Applicable)

Action Item	Responsible	Timing	Notes
Prepare termination letter	HR/Legal	24 hrs before	State reason, effective date, benefits
Schedule termination meeting	HR	24 hrs before	Private location, have security available
Disable network access	IT Security	During meeting	AD account, VPN, all systems
Revoke physical access	Security	During meeting	Badge deactivation, facility lockout
Retrieve company property	HR/Manager	During meeting	Laptop, phone, badge, keys, documents
Remote access verification	IT Security	Within 1 hour	Confirm no active sessions
Email forwarding/out-of-office	IT	Same day	Forward to manager, set OOO message
Document exit	HR	Same day	Exit interview notes, property receipt
Final paycheck processing	HR/Payroll	Per law	Comply with state law requirements
COBRA notification	HR	Within 14 days	Health insurance continuation rights

9.3 Post-Termination Monitoring

After termination for insider threat, implement enhanced monitoring:

- Monitor for attempted account access (30 days minimum)
- Alert on any contact from ex-employee to current employees
- Watch for data access by associates/friends still employed
- Review competitive intelligence for signs of data misuse
- Monitor job postings at competitor (confirm employment)
- Track any public disclosures or social media posts
- If data theft suspected, coordinate with customer contracts to watch for misuse

9.4 Preventive Measures & Lessons Learned

- **Technical Controls:** Were existing controls adequate? Need for enhanced DLP, UEBA, privileged access management?
- **Detection Capabilities:** How was threat detected? Could it have been detected sooner? What SIEM rules should be added?
- **Access Management:** Did subject have excessive access? Review least privilege principles, access certification process.
- **Policy Gaps:** Were policies clear? Did subject acknowledge policies? Update AUP, data handling, or remote work policies?
- **Training Needs:** Security awareness shortcomings? Manager training on behavioral indicators? Incident response training for investigators?
- **Process Improvements:** Investigation delays or bottlenecks? Improve HR-Security-Legal coordination?
- **Departing Employee Procedures:** If threat occurred during/after resignation, strengthen off-boarding process, immediate access restriction upon notice.
- **Insider Threat Program:** Formalize insider threat program with dedicated resources, cross-functional team, regular risk assessments.

10. Appendices & Templates

Appendix A: Investigation Report Template

1. Executive Summary (2-3 paragraphs)
2. Case Information (Case ID, dates, investigators, subject details)
3. Allegation Summary (What prompted investigation)
4. Investigation Scope & Methodology
5. Timeline of Events (detailed chronology)
6. Evidence Summary (organized by type)
7. Witness Interviews (summaries of key statements)
8. Technical Findings (SIEM analysis, AD review, forensics)
9. Subject Interview Summary (if conducted)
10. Analysis & Conclusions
11. Recommended Actions
12. Appendices (evidence exhibits, logs, supporting docs)

Appendix B: Key Investigation Forms

- **Case Intake Form:** Initial allegation documentation, severity assessment, team assignment
- **Investigation Plan:** Scope, objectives, timeline, resources, legal review
- **Evidence Log:** Chain of custody tracking for all collected evidence
- **Interview Consent Form:** Subject acknowledgment of interview, recording consent (if applicable)
- **Witness Statement Form:** Structured template for documenting interviews
- **Access Review Worksheet:** Document subject's access rights, justification review
- **Termination Checklist:** Ensure all termination tasks completed
- **Case Closure Report:** Final disposition, actions taken, lessons learned

Appendix C: Legal & Compliance Quick Reference

Topic	Key Considerations	Action Required
GDPR (EU)	Employee privacy rights Data minimization Legitimate interest basis	Legal review for EU employees Privacy impact assessment
CCPA (California)	Employee personal info protection Disclosure requirements	Check subject location Consult CA employment counsel
ECPA/SCA (US)	Email privacy Stored communications Consent requirements	Legal approval for email review Document business justification

Union Contracts	Weingarten rights Notice requirements Grievance procedures	Check collective bargaining agreement Union notification timing
Attorney-Client Privilege	Legal communications protected Crime-fraud exception	Legal counsel screens privileged material Privilege log
Trade Secret Protection	Inevitable disclosure Non-compete enforcement	Identify trade secrets involved Consider injunctive relief

Appendix D: Contact Information

Role	Name	Contact	Availability
General Counsel	[Name]	Email/Phone	24/7 for Critical cases
Employment Attorney	[Name/Firm]	Email/Phone	Business hours
HR Director	[Name]	Email/Phone	24/7 for Critical cases
CISO	[Name]	Email/Phone	24/7
SOC Manager	[Name]	Email/Phone	24/7
Digital Forensics Lead	[Name]	Email/Phone	On-call rotation
Privacy Officer	[Name]	Email/Phone	Business hours
Union Representative	[Name/Local]	Email/Phone	If applicable

REMINDER: Update contact information quarterly and after any personnel changes. Verify emergency contacts can be reached 24/7.

Document Control & Review

Review Cycle:	Quarterly or after each major investigation
Next Review Date:	[Date - 3 months from last update]
Document Owner:	SOC Manager / Legal Counsel
Approval Required:	CISO, General Counsel, HR Director
Distribution:	Strictly confidential - authorized personnel only
Retention:	Retain per legal hold and records retention policy

This playbook is a living document. Regular updates ensure alignment with evolving threats, legal requirements, and organizational changes. All personnel with access to this playbook must maintain strict confidentiality and use it only for authorized insider threat investigations.