CyberPeace

CYBERSECURITY POLICY GUIDE

FOR HUMAN RESOURCE DEPARTMENTS

A Governance and Implementation Framework Across the Employee Lifecycle

INTRODUCTION: WHY CYBERSECURITY HAS BECOME A CORE HR RESPONSIBILITY

Human Resources is not what it used to be. It has changed a lot because of technology. We do not use paper files or physical attendance registers anymore. Now we use cloud-based systems to manage resources track applicants and handle payroll. We also use portals for employees to access their information and tools to administer benefits. All these systems store data and in most companies it is Human Resources that is in charge of this data, not the IT department. This means Human Resources now handle a lot of personal data. An employee file can include their ID number, bank account details, salary history, performance reviews and health information. We also store data about job candidates, which includes a lot of information about people who may not even become employees. So we have to think about who can access this data, where it is stored and how it is moved between systems. This is not a Human Resources issue but also a cybersecurity issue.There are a lot of risks to this data.

According to a report by IBM the average cost of a data breach is around USD 4.44 million. The common way attackers get access to data is through phishing emails. Breaches caused by people inside the company can be very costly, around USD 4.92 million. Breaches caused by third-party companies can also be expensive, around USD 4.91 million. Human Resources is at risk because we use a lot of companies to handle payroll, background checks and recruitment. For Human Resources these risks can show up in ways. We can get phishing emails that look like they are about job offers or payroll. We can have problems with identity theft through job candidates or fake video interviews. We can also have problems with employees who still have access to data after they change jobs. Because Human Resources is in charge of creating, changing and ending employee identities a mistake in any of these areas can lead to access to company data. Artificial intelligence is becoming a part of Human Resources. It is used to screen resumes, schedule interviews and communicate with job candidates. While these tools can make our jobs easier they also store a lot of data. This can be a problem if we do not have security measures in place.

According to IBM using intelligence without proper governance can add around USD 670,000 to the cost of a data breach. We also have to think about fairness and accountability when using intelligence to make decisions about hiring and promotion.

CLOUD-BASED SYSTEMS

EMPLOYEE DATA

PHISHING RISKS

THIRD-PARTY VENDORS

AI IN HR

	STATISTIC	SOURCE	RELEVANCE TO HR
	Global average cost of a data breach: USD 4.44 million (2025)	IBM Cost of a Data Breach Report, 2025	Sets the financial stake behind every control in this guide
	Phishing is the leading initial attack vector, involved in roughly 16% of breaches	IBM Cost of a Data Breach Report, 2025	HR inboxes are a prime phishing target (fake offer letters, payroll requests)
	Malicious insider incidents average close to USD 4.92 million, the costliest breach category	IBM Cost of a Data Breach Report, 2025	Reinforces the case for the insider threat controls in Section 9
	AI use across HR tasks roughly doubled, reaching about 43% of organizations in 2025	SHRM 2025 Talent Trends survey	Makes AI governance (Section 7) a mainstream, not edge-case, concern
	Shadow AI was a factor in about 20% of breaches, adding roughly USD 670,000 to cost	IBM Cost of a Data Breach Report, 2025	Underscores the need for an AI tool inventory and approval process

DOCUMENT PURPOSE AND STAKEHOLDERS

This guide defines cybersecurity governance and implementation practices for Human Resource functions across the complete employee lifecycle from recruitment through separation. It is designed to serve simultaneously as a governance document (defining accountability and policy intent) and a practical implementation guide (providing procedures, checklists, and controls that can be adapted directly into organizational practice).

TARGET STAKEHOLDERS

- **Human Resources Department**
- **Chief Information Security Officer (CISO) and Security Team**
- **Information Technology Department**
- **Legal and Compliance Team**
- **Department Managers**
- **Executive Leadership**

Objective

This guide helps HR and related stakeholders understand their cybersecurity responsibilities throughout the entire employee lifecycle, from recruitment to employee exit, and provides organizations with a framework they can readily adapt to their own HR cybersecurity governance structure.

Scope and Applicability

This guide is written to remain valid across organizations of different sizes, sectors, and maturity levels. Three design principles govern how every control in this document is written.

1. **Organizational Size Tiers** Every control in this guide is presented with implementation guidance scaled to three organizational tiers, so that the same document remains usable whether an organization has ten employees or ten thousand.

Tier	Employee Count	Typical HR Reality
Small	Up to 50	One HR generalist, no dedicated Security function, limited HRMS budget
Mid-size	50 – 500	Dedicated HR team, some IT support, basic HRMS in place
Large / Enterprise	500+	Dedicated CISO, HR Business Partners, mature compliance function

2. INDUSTRY NEUTRAL PRINCIPLE

Controls in this guide are framed around data sensitivity and role type rather than industry sector, so that the same control language is directly usable by a hospital, a bank, a manufacturing company, or a software firm without modification. Organizations are regulated sectors banking and financial services, healthcare, and critical infrastructure should treat this guide as a baseline and layer any sector-specific obligations on top of it.

3. INDIAN LEGAL CONTEXT

This guide is grounded in the Indian legal and regulatory environment. The following statutes and frameworks are referred throughout:

- Digital Personal Data Protection Act, 2023 (DPPD Act) and the DPDP Rules, 2025 that is India's primary data protection framework
- Information Technology Act, 2000 - governing reasonable security practices
- The four Labour Codes Wage Code, Industrial Relations Code, Occupational Safety, Health and Working Conditions Code, and Social Security Code
- Prevention of Sexual Harassment (POSH) Act, 2013 relevant to reporting-channel design
- State-specific Shops and Establishments Acts relevant to records retentionminimums, which vary by state

This guide references the Digital Personal Data Protection Act, 2023 as India's primary data protection framework. As of 2026, DPDP obligations are in a phased rollout, with full enforcement beginning 13 May 2027. Where this guide describes a control as a "DPPD requirement," it reflects the Act's direction even where the specific implementing rule is still pending notification organizations should treat this as a compliance runway for building controls now, not a deadline to wait for.

The Data Protection Board of India was established with effect from 13 November 2025, the date on which the DPDP Rules, 2025 were also noted. Provisions relating to Consent Managers are scheduled to take effect around 13 November 2026, and full substantive compliance obligations become enforceable from 13 May 2027. Certain areas including cross-border data transfer restrictions and Significant Data Fiduciary designation remain pending separate government notification as of early 2026. Organizations should verify current implementation status against the Government's official notifications before finalizing compliance-dated claims (see References).

1. Understanding the DPD Act: A Practical Primer for HR

Why This Matters

HR is one of the largest internal generators and users of personal data in most organizations, covering employees, candidates, dependents, and sometimes contractors. Under the Digital Personal Data Protection Act, 2023 (DPPD Act), the organization itself is legally responsible for how that data is collected, used, stored, shared, and, HR is very often the function actually carrying out that processing day to day. This section is not a substitute for legal advice; it exists to give HR practitioners a working vocabulary so that conversations with Legal, IT, and Security about DPDP compliance start from a shared understanding.

Key Concepts

The DPDP Act is built around a small set of defined roles and terms that recur throughout the Act and throughout this guide. Understanding who is who, in the Act's own language, is the starting point for everything else, from the consent notices HR sends candidates to the vendor contracts HR signs with recruitment agencies and HRMs providers.

Term	What It Means	HR Relevance
Data Principal	The individual to whom the personal data relates. For HR purposes, this is the employee, the candidate, or occasionally a dependent.	Every consent notice, access request, and grievance channel in this guide is written from the Data Principal's perspective.
Data Fiduciary	The person or organization that determines the purpose and means of processing personal data. In an employment relationship, this is the employer itself.	The organization, not HR as a department, carries the legal obligations; HR executes many of them in practice.
Data Processor	A third party engaged by the Data Fiduciary to process personal data on its behalf, under a contract.	Payroll bureaus, background check vendors, and cloud HRMS providers are typically Data Processors; HR's vendor contracts should say so explicitly.
Significant Data Fiduciary (SDF)	A category of Data Fiduciary may designate based on factors such as the volume and sensitivity of data processed, triggering extra obligations.	Large employers with extensive workforce and candidate databases should monitor whether they may be designated an SDF as this provision is notified.
Personal Data	Any data about an individual who is an identifiable by or in relation to that data.	Covers nearly everything that holds: names, IDs, salary, health data, performance records, even biometric attendance logs.
Consent Manager	A registered intermediary through which a Data Principal can give, manage, and withdraw consent across multiple Data Fiducaries.	Not yet a routine requirement for most employers; relevant mainly to platforms that aggregate consent across many services.

In practice, most HR teams will interact with three of these terms constantly: the organization is the Data Fiduciary, the employee or candidate is the Data Principal, and any outsourced vendor handling that data on the organization's behalf is a Data Processor. Getting this triangle right in contracts and consent language is one of the most useful DPDP habits an HR team can build.

Consent and “Legitimate Uses” in the Employment Context

The DPDP Act generally requires free, specific, informed, and unambiguous consent before personal data is processed. Section 7 of the Act, however, sets out a closed list of “legitimate uses” where processing is permitted without separate consent. Section 7(i) is directly relevant to HR: it permits an employer to process personal data for the purposes of employment, including safeguarding the employer from loss or liability such as preventing corporate espionage, protecting trade secrets and intellectual property, and providing services or benefits an employee has requested. This is a narrower exemption than it may sound. Legal commentary generally reads it as covering the ongoing employment relationship rather than open-ended, indefinite use of former employees' data, and it does not remove HR’s other obligations around data minimization, security, and retention. Where processing goes beyond what Section 7(i) plausibly covers, such as most pre-employment and recruitment activities, HR should default to seeking consent and issuing a clear notice, and should involve Legal in drawing that line rather than assuming the exemption applies.

Data Fiduciary Obligations That Touch HR Directly

- Notice and consent: any consent-based collection must be accompanied by a clear notice describing what data is collected and why.
- Data accuracy: personal data used for decisions likely to affect the individual must be kept accurate and complete.
- Retention and erasure: personal data should be erased once its purpose is served, unless retention is required by another law — this is the legal backbone behind the retention schedules described in Section 5.
- Breach notification: the organization must notify the Data Protection Board of India and affected individuals in the event of a personal data breach, in the manner the Rules prescribe — this underpins the incident-response obligations described in Section 11.
- Grievance redress: the organization must maintain an effective mechanism for Data Principals to raise concerns about how their data is processed.

WHAT THIS MEANS IN PRACTICE

When HR signs a contract with a payroll bureau, background-check vendor, or recruitment platform, that contract should identify the vendor as a Data Processor, specify the purpose and limits of processing, and require the vendor to support the organization's breach-notification and ensure obligations. Where HR issues consent notices to candidates or employees, those notices should be specific about purpose rather than generic, and should not bundle unrelated uses into a single consent. For the current phased implementation timeline and enforcement dates, see the Indian Legal Context note earlier in this guide and the References section.

2. GOVERNANCE AND ROLES

Why This Matters

HR sits at the intersection of the organization's most sensitive data and its highest-risk processes onboarding and offboarding directly control system access. Most HR-related security failures occur not because a control did not exist, but because no one was clearly accountable for executing it.

Governance Structure

- Small organizations: one individual (often the HR head or founder) holds joint HR-security accountability; a lightweight quarterly checklist review substitutes for a formal committee.
- Mid-size and large organizations: a named HR-Security Liaison attends regular security syncs; a cross-functional HR Security Working Group (HR, IT, Security, Legal, and a rotating Department Manager) meets quarterly to review policy, incidents, and audit findings.
- At every size: new HR technology, AI tools, or third-party vendors require joint sign-off from HR, IT/Security, and Legal before procurement not after.

RACI MATRIX - GOVERNANCE FUNCTIONS

Activity	HR	CISO / Security	IT	Legal	Managers	Executive
Define HR security policy	A/R	C	C	C	I	I
Approve HR technology / vendors	R	A	C	C	I	I
Onboarding / offboarding execution	R	C	A	I	C	I
Employee data classification	A/R	C	C	C	I	I
Insider threat investigations	C	A/R	C	C	I	I
Incident response (HR data)	C	A	R	C	I	I
Compliance audits	R	C	C	A	I	I
Security awareness training	R	A	C	I	C	I

R = Responsible *A = Accountable* *C = Consulted* *I = Informed*

Sample Policy Statement

HR is accountable for submitting access provisioning, modification, and revocation requests accurately and promptly upon a triggering employment event. IT is accountable for executing these requests within a defined service level and confirming completion in writing. In small organizations without a formal ticketing system, this confirmation may take the form of a signed checklist.

2. RECRUITMENT AND CANDIDATE MANAGEMENT

Why This Matters

Recruitment pipelines have become an active attack surface: fraudulent candidates seeking insider access, deepfake video interviews, resume-borne malware, and phishing disguised as offer letters are all documented attack patterns.

Applicant Data Handling

Collect only the data necessary for the role under evaluation (data minimization); avoid default 'collect everything' Applicant Tracking System (ATS) configurations.

Small organizations: store applicant data in access-restricted folders or spreadsheets, with a manual, calendar-based deletion reminder for rejected candidates.

Mid-size and large organizations: use an ATS with role-based access controls and automated retention and deletion rules.

Identity and Background Verification

Verify government-issued identification against a live selfie or video check for remote hires, particularly for information technology or privileged roles.

For final-round video interviews, require live, unscripted interaction for example, asking candidates to perform a simple physical action on camera as a deepfake detection technique. This is feasible at any organizational size and requires no additional tooling.

Cross-check candidate-provided details independently rather than relying solely on documents supplied by the candidate.

Anti-Fraud Controls

Threat	Red Flag	Control
Fake candidate / insider placement	Reluctance to appear live on video	Mandatory live video final round
Phishing via fake recruiter	Urgent offer; request for bank details before Day 1	Publish and verify official recruiter domains
Resume-borne malware	Unusual file types submitted as a “resume”	Restrict and scan file types at intake
Recruitment platform compromise	Bulk data export anomalies	MFA and logging on all ATS / vendor accounts

Third-Party Recruitment Agencies

Require a signed data handling agreement specifying breach notification timelines and deletion obligations even a one-page agreement for a small organization is materially better than no agreement. Limit agency access to only the requisitions they are actively working on.

3. Employee Onboarding

Why This Matters

Onboarding is the point at which the principle of least privilege is either established or lost. Over-provisioning on Day 1 granting a new hire whatever the previous person in that role happened to have is one of the most common sources of excess access later flagged in audits.

Standard Operating Procedure - Secure Onboarding

Pre-Day 1: HR submits a role-based access request against a pre-approved access template for that job title (a documented list per role for small organizations; an automated template within the HRMS or identity provider for larger organizations).

Identity verification is completed before any credentials are issued.

Account provisioning is executed strictly against the approved template; any deviation requires manager and security sign-off.

Multi-factor authentication (MFA) is enrolled before first login to any system containing sensitive data.

Security awareness training is completed before production system access is granted even where this introduces a short delay.

Devices issued are encrypted and endpoint-protected; personal device use requires enrollment in mobile device management (MDM) under a documented BYOD policy.

Signed acknowledgments acceptable use, data protection, and confidentiality agreements are logged and retained.

Checklist: Onboarding Security Gate

- [ ] Identity verified
- [ ] Access matches the approved role template
- [ ] MFA enrolled
- [ ] Security awareness training completed
- [ ] Device encrypted and endpoint-protected
- [ ] Signed policy Acknowledgments on file
- [ ] Manager confirms access matches actual job duties (30-day review)

4. Employee Data Protection

Why This Matters

HR holds some of the most sensitive personal data in the organization health records, disciplinary history, salary details, and immigration status among them. A breach in this domain carries regulatory, reputational, and personal harm consequences simultaneously.

Data Classification Model

Tier	Examples	Controls
Restricted	National ID, health records, background check results, disciplinary records	Encrypted, access logged, need-to-know only, MFA required
Confidential	Salary, performance reviews, home address	Role-based access, encrypted, access logged
Internal	Org charts, general HR policies	Employee-accessible, standard controls
Public	Job postings, published policies	No special controls

CORE CONTROLS

- **Encryption:** applied at rest and in transit. Small organizations can rely on built-in encryption offered by mainstream cloud providers, often included at no additional cost; larger organizations should implement dedicated key management.
- **Access control:** role-based, reviewed periodically, with access reviews triggered automatically by any role change.
- **Retention and disposal:** retention periods should be defined by data type. Shops and Establishments Actminimums vary by Indian state confirm the applicable state requirement rather than assuming a single national figure. Records past their retention period should be securely deleted or disposed of.
- **Cross-border transfers:** monitor the DPDP Act's evolving restricted-country provisions, as this area remains pending separate government notification.
- **Sensitive data:** segregate storage, restrict access to named HR and Legal personnel, and log every access event.

SAMPLE POLICY STATEMENT

Employee personal data classified as Restricted may only be accessed by named HR and Legal personnel on a need-to-know basis. All such access is logged and subject to periodic review, consistent with the organization's obligations as a Data Fiduciary under the Digital Personal Data Protection Act, 2023.

5. HR SYSTEMS AND TECHNOLOGY

This section applies to HR Management Systems (HRMS), payroll systems, recruitment portals, attendance systems, cloud platforms, and third-party HR applications.

Vendor due diligence: prefer vendors holding recognized security certifications, such as ISO or SOC 2. Where a full audit is not feasible, a basic security questionnaire is a reasonable minimum for smaller organizations.

- **Configuration:** enforcement single sign-on (SSO) and MFA on all HR platforms; disable legacy authentication protocols.
- **Segregation of duties:** the individual who can change payroll bank details should not be the same individual who can approve that change.
- **Logging:** centralize HR system logs and alert on bulk exports and off-hours access. Small organizations can conduct periodic manual log review; larger organizations should integrate logs with a Security Information and Event Management (SIEM) platform.
- **API integrations:** audit third-party application integrations connected to the HRMS and revoke unused access tokens.

6. AI Usage in HR

Why This Matters

Artificial intelligence is now embedded in resume screening, chatbot interviews, and performance analytics frequently introduced without security or legal review ("shadow AI"), creating bias, privacy, and data-leakage risk.

Governance

Acceptable Use

AI may assist screening, drafting, and analysis, but must not be the sole basis for hiring, promotion, disciplinary, or termination decisions. A qualified human decision-maker must review, and be able to override, every AI-influenced outcome.

Prohibited Practices

- Using AI to infer protected characteristics that have not been voluntarily disclosed.
- Fully automated rejection of a candidate without human review.
- Undisclosed use of AI-generated content where disclosure is legally required.

Bias Mitigation

Periodic bias audits of AI screening tools should be conducted and documented, with Legal review, alongside a human appeals process for any AI-influenced decision.

Data Protection

Confirm whether an AI vendor trains its models on organizational data, and require a contractual opt-out where this is the case. The same data classification and retention rules applied to source data should apply equally to AI-generated logs and outputs.

Sample Policy Statement

No AI tool may be used to make a final hiring, promotion, or termination decision. All AI-assisted recommendations must be reviewed by a qualified human decision-maker, and that review must be documented.

7. PAYROLL AND FINANCIAL FRAUD PREVENTION

COMMON FRAUD PATTERNS AND CONTROLS

Scenario	Description	Control
CEO impersonation	Spoofed email requesting an urgent wire transfer or gift cards	Out-of-band verification for any payment request from leadership
Bank account change fraud	Email requesting a payroll bank detail change	Mandatory callback verification to a known phone number before any change
Salary record tampering	Insider or compromised account modifies salary data	Segregation of duties: initiator and approver must differ
Tax document phishing	Mass email requesting employee tax documents	Restrict bulk PII export; verify requester identity independently

STANDARD CONTROL: BANK DETAIL CHANGE PROCEDURE

- ☑ **Change request is received through any channel – no action is taken at this stage.**
- ☑ **HR calls the employee back on the phone number already on file, never a number supplied in the request.**
- ☑ **The change is processed only after verbal confirmation.**
- ☑ **A confirmation is sent to the employee's original registered address, inviting an immediate report if the change was unauthorized.**

This procedure is identical at any organizational size , it requires a phone call, not a technology investment.

8. Insider Threat Management

Framewo

Privileged Access

Maintain a register of employees holding elevated access and review it periodically together with their managers.

Behavioral Indicators (For Awareness, Not Automated

- Sudden interest in data or systems outside the employee's normal job scope.
- Attempts to access former colleagues' accounts.
- Unusual data transfer patterns flagged by IT or Security.

Reporting

Maintain a confidential channel for concerns, rooted jointly to HR and Security. Security leads technical detection; HR manages the employment process; Legal reviews before any action affecting employment status is taken.

Privacy

Monitoring of employee systems for insider threat purposes must be proportionate, documented, and limited to legitimate security purposes. Any investigation involving an employee's personal communications requires Legal sign-off and, where required by law, employee notification.

9. EMPLOYEE LIFECYCLE SECURITY

COVERAGE ACROSS LIFECYCLE EVENTS

EVENT	KEY SECURITY ACTIONS	OWNER
Internal transfer / promotion	Full access re-review against the new role; revoke access no longer needed	**HR + IT**
Extended leave	Suspend, rather than delete, access	**HR + IT**
Contractor / temporary staff	Time-bound accounts with a hard expiry date; sponsoring manager is accountable	**HR + Manager**
Remote employees	VPN or zero-trust access; home network baseline security guidance	**IT + HR**

OFFBOARDING - FULL CONTROL SET

Offboarding is the single highest-risk moment in the employee lifecycle. Once separation is decided, the gap between “decision made” and “access removed” is pure exposure. Each control below is written using a consistent structure the underlying principle, its implementation at small and at mid/large organizations, the accountable owner, and how it can be independently verified.

1 CONTROL 1 - ACCESS REVOCATION TIMING

Principle: System access must be revoked at the moment separation is confirmed not at end of day, and not queued behind routine IT tickets. For involuntary separations, revocation must occur simultaneously with, or immediately before, the employee is informed.

- **Small organization:** HR notifies the designated IT or admin contact directly by phone or in person never by email alone. A starting manual checklist covers every system requiring deactivation, signed off the same day.
- **Mid/large organization:** an HRMS status change automatically triggers a deprossiving workflow across integrated systems. Non-integrated systems are covered by a service-level-bound ticket with automatic escalation.
- **Owner:** HR (trigger and notification) and IT (execution), jointly accountable.
- **Verification:** compare thetimestamp of separation confirmation against thetimestamp access was disabled, across a sample of recent separations. The gap should be near-zero.

2 CONTROL 2 - ASSET RECOVERY

Principle: All company-issued physical and digital assets laptops, phones, access badges, security tokens, storage devices must be covered and logged before final settlement is processed, wherever local law permits linking recovery to final pay.

- **Small organization:** a simple asset register (spreadsheet) is checked off as items are physically returned, in person, on or before the last working day.
- **Mid/large organization:** asset recovery is tracked through an IT asset management system linked to the HRMS record, with remote lock or wipe triggered independently of physical recovery.
- **Owner:** HR (tracking and escalation) and IT (technical lock or wipe).
- **Verification:** confirm a completed, signed asset checklist, or a wipe Confirmation log, exists for every sampled separation.

3 CONTROL 3 - CREDENTIAL ROTATION

Principle: Any shared, service, or system account the departing employee had access to or knowledge of must have its credentials rotated as part of offboarding deactivating the individual's own account is not sufficient on its own.

- **Small organization:** a manual list of shared login's the employee had access to is maintained; the designated IT/admin contact resets these passwords the same day.
- **Mid/large organization:** a privileged access register drives automatic or checklist-based rotation, validated by Security for high-privilege accounts.
- **Owner:** IT/Security (execution) and HR (identifying which accounts applied to the employee).
- **Verification:** confirm a privileged/shared access register exists, was consulted at separation, and that rotation timestamps precede or match the employee's last working day.

4 CONTROL 4 - EMAIL AND MAILBOX HANDLING

Principle: **Mailbox access must be limited, time-bound, and policy-defined full, indefinite access for a manager is not an acceptable default.**

Small organization: an auto-reply plus forwarding of specific, pre-identified business threads to the manager for a fixed period, after which the mailbox is disabled or archived.

Mid/large organization: the mailbox is placed on a legal or administrative hold per the retention policy, with time-limited delegated access granted, and automatic archival or deletion once the hold period lapses.

Owner: IT (technical control) and HR (defining access duration per policy).

Verification: confirm that no former employee's full mailbox login remained active or shared beyond the policy-defined window.

5 CONTROL 5 - EXIT INTERVIEW: SECURITY COMPONENT

Principle: **Every exit interview must include a security-specific segment — reiterating ongoing confidentiality obligations, confirming removal of company data from personal devices where BYOD was used, and collecting any physical documents or notes.**

Small organization: a short standard checklist during the exit conversation, with a signed acknowledgment.

Mid/large organization: the same checklist embedded in a formal offboarding workflow, with mobile device management-confirmed removal of company data from personal devices.

Owner: HR (conducts and documents) and IT (technical BYOD confirmation, where applicable).

Verification: confirm a signed exit acknowledgment exists for each sampled separation, recording both the confidentiality reminder and the device-data removal confirmation explicitly.

6 CONTROL 6 - HIGH-RISK SEPARATION FLAG

Principle: **Involuntary separations, termination for cause, layoffs, disputed exits — require enhanced monitoring during the notice period and tighter coordination between HR, Security, and Legal, proportionate to risk rather than routine surveillance.**

Small organization: HR flags the case to the IT/admin contact in advance where legally possible, so access is revoked at the exact moment of notification.

Mid/large organization: HR flags the case to Security in advance, under Legal's guidance, enabling simultaneous access revocation and, where policy and law permit, temporary, time-bound, and documented heightened logging strictly for the remaining notice period.

Owner: HR (flagging and timing), Security (monitoring, where applicable), and Legal (approval and boundaries).

Verification: confirm a documented decision exists on the timing of notification versus access revocation, and that any enhanced monitoring applied was time-bound, logged, and had Legal sign-off.

Offboarding - Roles and Responsibilities (RACI)

Control	HR	IT	Security	Legal	Manager
Access revocation timing	R	A	C	I	I
Asset recovery	R	A	I	I	C
Credential rotation	C	A	R	I	I
Email / mailbox handling	C	A	I	C	C
Exit interview (security)	A/R	C	I	I	I
High-risk separation flag	R	I	A	A	I

R = Responsible **A** = Accountable **C** = Consulted **I** = Informed

Offboarding Master Checklist

- [ ] Separation confirmed and logged with a timestamp
- [ ] Access revocation aligned with, or ahead of, notification for involuntary exits
- [ ] All systems, including SaaS and cloud platforms, confirmed disabled
- [ ] Assets recovered and logged
- [ ] Shared or service credentials rotated
- [ ] Mailbox access time-bound and documented
- [ ] Exit interview security checklist completed and signed
- [ ] High-risk cases flagged with a documented monitoring decision

10. INCIDENT RESPONSE - HR'S ROLE

Escalation Flow

1. Incident detected or reported
2. Is it employee-data-related or insider-related?
3. If yes, HR notifies the CISO/Security promptly
4. Security leads the technical investigation while HR leads the employee-facing process and Legal assesses notification obligations
5. A joint decision is made on containment, communication, and any disciplinary or legal action
6. A post-incident review updates policy.

HR Responsibilities by Incident Type

- **Credential compromise:** confirm identity, support the reset process, and monitor for related HR process abuse.
- **Insider threat confirmed:** coordinate with Legal on employment action, preserve documentation, and manage internal communication carefully.
- **Data breach involving employee PII:** support Legal and Security in identifying affected individuals and drafting notifications. Under the DPDP Act, breach notification to the Data Protection Board and affected individuals is expected within a short defined window organizations should confirm the current timeline against the DPDP Rules as further provisions are notified.
- **Ransomware affecting HR systems:** support business continuity, including manual payroll processing and alternate communication channels

11. SECURITY AWARENESS AND TRAINING

Audience	Core Content	Frequency
All employees	Phishing, password hygiene, social engineering, data handling	Onboarding + annual refresh
HR personnel	Candidate fraud, deepfake awareness, PII handling, AI tool usage, payroll fraud red flags	Onboarding + biannual
Managers	Insider threat indicators, secure offboarding participation	Annual
Executives	Business email compromise / whaling awareness, incident response role	Annual, tabletop exercises

Small organizations can deliver this content through short, low-cost sessions such as recorded videos and simple quizzes. Mid-size and large organizations can invest in simulated phishing campaigns and formal learning-management-system tracking.

12. COMPLIANCE AND RISK MANAGEMENT

FRAMEWORK MAPPING

Guide Section	ISO 27001	NIST CSF	Indian Regulatory Hook
Governance & Roles	A.5	GOVERN	Corporate governance norms
Access control	A.8, A.5.15–5.18	PROTECT (PR.AC)	—
Data protection	A.5.34, A.8.24	PROTECT (PR.DS)	DPDP Act, 2023 & DPDP Rules, 2025
Incident response	A.5.24–5.28	RESPOND, RECOVER	DPDP breach notification obligations
Risk assessment	Clause 6.1, A.5.7	IDENTIFY	Sector-specific requirements, as applicable

RISK MATRIX (ILLUSTRATIVE)

Risk	Likelihood	Impact	Priority
Delayed offboarding access revocation	High	High	Critical
Payroll business email compromise fraud	Medium	High	Critical
Unvetted AI tool used on candidate data	Medium	Medium	High
Over-privileged onboarding	High	Medium	High

Risk	Likelihood	Impact	Priority
Insider data exfiltration before resignation	Low	High	Medium

REVIEW CADENCE

- **Quarterly:** access reviews, an offboarding audit sample, and phishing simulation results for mid-size and large organizations; a simplified quarterly checklist review for small organizations.
- **Annual:** a full policy review, a framework gap assessment, and a DPDP compliance status check against the Government's implementation tracker, as rules continue to be notified in phases through 2027.

Implementation Roadmap (0-12 Months)

Months 1-2: Foundation

Establish governance ownership; document current access, data flows, and vendors; conduct a gap assessment against this guide.

Months 3-5: Core Controls

Implement role-based access templates; deploy MFA; formalize same-day offboarding revocation; implement the payroll callback_verification control.

Months 6-8: Data and AI Governance

Complete data classification across HR systems; establish an AI tool inventory and approval process; update retention schedules against applicable state and DPPD requirements.

Months 9-10: Training and Insider Threat

Roll out tailored awareness training; establish the insider threat reporting channel and joint HR/Security/Legal review process.

Months 11-12: Audit and Maturity

Conduct the first full audit against the ISO 27001/NIST mapping; run a tabletop incident response exercise; brief Executive Leadership on residual risk and the roadmap for the following year.

References

- https://cadp.in/resources/guides/dpdp-implementation-tracker/
- https://www.amsshardul.com/insight/enforcement-of-the-dpdp-act-and-notification-of-the-dpdp-rules/
- https://www.fisherphillics.com/en/insights/indias-new-data-priority-rules—are here
- https://www.india-briefing.com/news/india-dpdp-compliance-timeline-enforcement-2026-27-4740.html
- https://www.glocertinternational.com/resources/guides/dpdp-act-and-rules-overview/
- https://www.lexology.com/library/detail.aspxg?=2073ac40-628f-4112-8113-fff1d4b8588
- https://www.fortra.com/blog/what-indias-digital-personal-data-protection-act
- https://www.dlapiperdataprotection.com/?=law&c=In
- https://www.riresponsibleailabs.ai/knowledge-hub/articles/india-dpdp-act-2026-2027
- https://www.atlassystems.com/blog/digital-personal-data-protection-act-india

CyberPeace

CYBERSECURITY POLICY GUIDE FOR HUMAN RESOURCE DEPARTMENTS

A Governance and Implementation Framework Across the Employee Lifecycle

Contributor: Ritika Goswami, Intern, Policy & Advocacy, CyberPeace