SECTION 1. WORKING HOURS & ATTENDANCE

1.1 Standard Schedule: All full-time employees are expected to work a 40-hour week, Monday through Friday, 9:00 AM – 5:00 PM local time with a 60-minute unpaid lunch break.

1.2 Core Collaboration Window: 10:00 AM – 3:00 PM local time. Employees must be online, reachable, and capable of joining meetings during this window.

1.3 Flexible Start: Employees may start any time between 7:30 AM and 9:30 AM provided they satisfy the core window; schedule changes beyond two consecutive weeks must be updated in the shared team calendar.

1.4 Breaks: Two paid 15-minute wellness breaks are encouraged (one before lunch, one after). Breaks should not be accumulated or converted to additional leave.

1.5 Overtime: Must be pre-approved in writing by a manager. Unauthorized overtime may not be compensated.

1.6 Remote Punctuality: Remote employees must signal daily presence via the collaboration platform status by 9:15 AM.

SECTION 2. HYBRID & REMOTE WORK

2.1 Eligibility: Roles classified as "Onsite Essential" must perform at least 4 days onsite; others may adopt hybrid (minimum 2 days onsite) or full remote upon VP approval.

2.2 Remote Equipment: Company-issued laptop, security key, and approved peripherals are required. Personally owned storage devices are prohibited.

2.3 Workspace Security: Remote workers must use a private, distraction-minimized area. Family/shared spaces are acceptable only if screen privacy filters are used.

2.4 Network Standards: All remote access to corporate systems MUST route through the corporate VPN with MFA. Public Wi-Fi is permissible only if connected through VPN; tethering from unsecured mobile hotspots is prohibited.

2.5 Travel Notification: Any planned remote work from a new country must be declared at least 10 business days in advance.

SECTION 3. INFORMATION SECURITY

3.1 Classification: Data is categorized as PUBLIC, INTERNAL, CONFIDENTIAL, or RESTRICTED. Handling requirements scale with sensitivity.

3.2 Storage: CONFIDENTIAL or RESTRICTED data must only reside in approved encrypted repositories. Local desktop storage of RESTRICTED data is forbidden.

3.3 Transmission: RESTRICTED data transmission requires end-to-end encryption; email attachments must be password protected with a separate channel delivery of the passphrase.

3.4 Passwords: Minimum length 14 characters; must include at least 1 uppercase, 1 lowercase, 1 number, and 1 symbol. Password reuse across systems is prohibited.

3.5 MFA: Mandatory for VPN, email, code repositories, admin consoles, and any system with production data.

3.6 Device Hardening: Operating system patches must be applied within 7 days of release for critical vulnerabilities and 30 days for high severity.

3.7 Logging & Monitoring: Access logs for production systems retained 400 days. Security events escalated to SecOps within 30 minutes of detection.

3.8 Removable Media: Use of USB storage devices is disallowed unless explicitly approved and hardware-encrypted.
3.9 Incident Reporting: Any suspected breach must be reported within 1 hour via the Security Hotline channel.

SECTION 4. DATA PRIVACY & RETENTION
4.1 PII Handling: Personally Identifiable Information must be encrypted at rest (AES-256) and in transit (TLS 1.3+). Decryption keys stored in a managed KMS with access auditing.
4.2 Data Minimization: Collection of PII must be limited to specific, documented business purposes. Quarterly reviews audit unused fields.
4.3 Subject Requests: Data subject access / deletion requests must be fulfilled within 25 days unless legally extended.
4.4 Retention: Customer transaction records retained 7 years then purged. Support chat logs retained 18 months. System error logs retained 12 months. Encrypted backups retained 90 days rolling.
4.5 Anonymization: Analytical exports must remove direct identifiers and apply tokenization for quasi-identifiers.
4.6 Cross-Border Transfer: RESTRICTED data may not leave approved jurisdictions without DPO authorization.

SECTION 5. ACCEPTABLE USE & SOFTWARE
5.1 Authorized Software: Only software from the managed application catalog may be installed. Exceptions require Security review.
5.2 Personal Use: Reasonable personal browsing (≤30 min/day) allowed if it does not consume excessive bandwidth or breach content standards.
5.3 Prohibited Activities: Crypto mining, dark web access, license circumvention, and peer-to-peer file sharing.
5.4 Open Source: Use must comply with license obligations; copyleft components in distributed binaries need Legal approval.
5.5 AI Tools: Only whitelisted AI assistants (see internal registry) permitted for source code or customer data. Copy-paste of RESTRICTED data into unapproved AI tools is a violation.

SECTION 6. PHYSICAL SECURITY
6.1 Badges: Must be worn visibly at all times onsite. Tailgating prevention is everyone's responsibility.
6.2 Visitors: Must sign NDA and be escorted. Visitor Wi-Fi network isolated from internal resources.
6.3 Secure Areas: Lab and data center access require biometric plus badge.

SECTION 7. HUMAN RESOURCES & CONDUCT
7.1 Anti-Harassment: Zero tolerance. All complaints investigated within 5 business days.
7.2 Performance Reviews: Conducted twice annually (mid-year & annual) with written feedback.
7.3 Training: Mandatory annual modules: Security Awareness, Code of Conduct, Data Privacy.

7.4 Gifts: Employees may accept non-cash items up to $50 fair market value per source per year.
7.5 Conflicts of Interest: Outside employment requiring >5 hrs/week must be disclosed.

SECTION 8. EXPENSES & TRAVEL
8.1 Booking: Domestic flights must be booked in economy class. Business class allowed only for international flights over 6 hours block time.
8.2 Submission: Expenses submitted within 30 days of incurrence; late submissions may be denied.
8.3 Receipts: Required for any single expense over $25.
8.4 Per Diem: Region-specific rates published quarterly on the Finance portal.

SECTION 9. CHANGE LOG
Initial issue for 2025 corporate baseline.