CYBER SECURITY:
STANDARD OPERATING PROCEDURE (SOP)

20 JUL 2026

INDEX

S No	Subject	Page No
—	Document Version History	i
1.	Cyber Security Standard Operating Procedure (Introduction, Aim, Objectives)	1
2.	Part I: Endpoint Hardening and Software Security	3
3.	Part II: Intra-Network Security	5
4.	Part III: Internet Security	6
5.	Part IV: Asset Management and Data Handling	7
6.	Part V: Physical and Environment Security	9
7.	Part VI: Audits and Incident Management	10
8.	Part VII: Digital Personal Data Protection (DPDP) Act 2023 Compliance	12
9.	Part VIII: PII and Health Data Protection	17
10.	Part IX: Protection of Children's Personal Data (Minor Beneficiaries)	20
11.	Part X: Cyber Incident Management and Reporting Procedure	23
12.	Part XI: Password Management Policy	30
13.	Part XII: Patch Management Policy	32
14.	Part XIII: Information Classification Policy	34
15.	Part XIV: Security Logging and Monitoring Policy	38
16.	Part XV: Software Development Life Cycle (SDLC) Policy	42
17.	Part XVI: Risk Assessment and Management Policy	49
18.	Annexure A – DPDP Consent Form (Adult Beneficiary)	54
19.	Annexure B – DPDP Consent Form (Minor Beneficiary / Guardian)	55
20.	Annexure C – Data Breach Response Protocol	56
21.	Annexure D – PII Data Classification Register	57
22.	Annexure E – Cyber Incident Report Format (Internal CIRF)	58
23.	Annexure F – CERT-In Cyber Security Incident Report Format	61

DOCUMENT VERSION HISTORY

CO ECHS — Cyber Security Standard Operating Procedure

File No: B/49722-IT/SOP/AG/ECHS

Version Control Policy

This document is subject to version control. No amendments shall be made to this SOP without the written authorisation of the Dir (Stats & Automation), CO ECHS. All revised versions shall be assigned a new version number, dated, and promulgated to all holders. Superseded versions must be recalled and destroyed within 30 days of promulgation of the revised version.

Version	Date	Status	Amended By	Summary of Changes	Approved By
v1.0	31 Dec 2024	Initial Release	Dir (Stats & Automation), CO ECHS	Original CO ECHS Cyber Security SOP covering: • Endpoint hardening and software security • Intra-network and internet security • Asset management and data handling • Physical and environment security • Basic audit and incident management	Col Anurag Bhardwaj Dir (Stats & Automation) CO ECHS
v2.0	2026	Current Version	Dir (Stats & Automation), CO ECHS	Major revision incorporating: • Part VII: DPDP Act 2023 compliance framework • Part VIII: PII and health data protection controls • Part IX: Children's data protection (DPDP S.9) • Part X: Full incident management lifecycle procedure • DPO appointment and data retention schedule • Consent forms (adult and minor) • CERT-In incident report format (Annexure F) • Internal CIRF format (Annexure E)	Col Anurag Bhardwaj Dir (Stats & Automation) CO ECHS
v3.0	Jun 2026	Current Version	Dir (Stats & Automation), CO ECHS	Added Parts XI–XV and Annexure G (Risk Assessment and Management Policy) comprising 8-section RAMP with 5x5 risk matrix,	Col Anurag Bhardwaj Dir (Stats & Automation) CO ECHS

				Likelihood/Impact definitions, 10-entry ECHS Risk Register, response and escalation table, and roles. Aadhaar Data Breach Reporting Form re-designated Annexure H. Part XI: Password Management Policy (paras 62–68). Part XII: Patch Management Policy (paras 69–75). Part XIII: Information Classification Policy (paras 76–82) with DPDP/Aadhaar/Health Records classification matrix. Para 35A: Log Retention Policy (2-year running / 5-year archival standard). Part XIV: Security Logging and Monitoring Policy (paras 83–90). Part XV: SDLC Policy for Vendor/Agency Software (paras 91–99) covering agency role definitions, procurement security requirements, Pre-Procurement Security Assessment, contractual obligations, secure deployment, vulnerability and patch management, security monitoring, software decommissioning, and compliance audit. Log retention periods updated across paras 13.5, 43, 46.4, 72, 75, 80, and Classification Matrix.	

Note: *Holders of this document are responsible for ensuring they hold the current version. Queries regarding version status should be directed to the Data Protection Officer, CO ECHS.*

CYBER SECURITY STANDARD OPERATING PROCEDURE (SOP)

Introduction

1. The increased dependence on cyberspace warrants an understanding of the challenges and threats linked with the cyber domain. With proliferation of IT, associated cyber threats have also increased at all levels. ECHS, as a health-care delivery organization, processes large volumes of sensitive Personally Identifiable Information (PII) including health records of retired defence personnel, their dependents, and minor beneficiaries — all of whom are entitled to special protection under Indian law. This SOP has been comprehensively updated to incorporate obligations under the **Digital Personal Data Protection (DPDP) Act 2023** in addition to existing cyber security requirements.

2. The concept of cyber security devolves upon **People, Process and Technology**. In order to ensure robust and resilient cyber security, we need to focus on people and processes while leveraging available technology. This SOP has been formulated in accordance with these tenets.

3. All IT assets of stakeholders under **ECHS** and personnel handling these resources will be governed by this cyber security policy. Contravention of any clause will be construed as a cyber-violation and may attract disciplinary action and/or penalties under the DPDP Act 2023. The SOP has been derived with reference to:

3.1 Information Technology Act 2000 and IT (Amendment) Act 2008.

3.2 Classification and Handling of Classified Documents – 2001.

3.3 National Cyber Security Policy – 2013.

3.4 Army Cyber Security Policy – 2023.

3.5 Digital Personal Data Protection (DPDP) Act 2023 (No. 22 of 2023).

3.6 DPDP Rules 2025 (as notified).

3.7 Ministry of Health & Family Welfare Guidelines on Electronic Health Records (EHR) 2023.

3.8 CERT-In Guidelines on Cybersecurity Incident Reporting.

Aim

4. To lay down Cyber Security Standard Operating Procedures (SOPs) for all stakeholders under ECHS, incorporating obligations related to the protection of Personal Data, Health Data, and the Data of Minor Beneficiaries under the DPDP Act 2023.

Objectives

5. The objectives of this document are:

5.1 Generate trust and confidence in ICT infrastructure facilitating exchange of operational and sensitive information without compromising security.

5.2 Ensure compliance with the DPDP Act 2023 in the processing, storage, and transfer of personal data of all ECHS beneficiaries.

5.3 Establish a lawful basis and consent framework for collection of health data from beneficiaries, including minors.

5.4 Refine overarching cyber security policies and procedures.

5.5 Lay down inherent responsibility and accountability for data fiduciaries.

5.6 Safeguard digital information and ensure its availability, integrity and confidentiality during storage, processing, transit and handling.

5.7 Create a culture of cyber security and responsible data handling through awareness, skill development, training and monitoring.

Inherent Responsibility and Accountability

6. The details of responsibility of major stakeholders are outlined below. Under the DPDP Act 2023, ECHS is classified as a **Data Fiduciary** and all Officers at various levels are responsible for ensuring compliance within their Areas of Responsibility (AOR):

6.1 OIC PC. The Officer in Charge of the Polyclinic (PC) will be responsible for implementation of cyber security policies at respective PC. Key areas of responsibility are highlighted in subsequent paragraphs.

6.2 OIC ECHS Cell (Station HQ). Officer in Charge at ECHS Cell (Stn HQ) will ensure implementation of cyber security policies at respective PC associated with Stn HQ.

6.3 Director RC. Dir RC will be overall responsible for implementation of cyber security policies at respective RC and all PCs under AOR.

6.4 Data Protection Officer (DPO). A designated DPO will be appointed at CO ECHS level to oversee DPDP Act 2023 compliance, handle Data Principal grievances, and liaise with the Data Protection Board of India.

PART I: ENDPOINT HARDENING AND SOFTWARE SECURITY

Hardware Security Management

7. Hardware Management

7.1 Inventory Management of IT Assets. Inventory of IT hardware and devices will be maintained by Cyber Security Officers/Network Administrators, duly nominated by Stn HQs for each PC. Logbooks for each IT asset will be maintained centrally by each unit/establishment.

7.2 Secure Disposal of Data. System logs, printouts, used printer ribbons, printer cartridges, damaged optical media, tapes and hard disks containing personal/health data must be disposed of securely using methods prescribed in Part VIII. Records of disposal will be maintained for equipment by respective PC/establishment.

7.3 Backup and Storage of Data. To prevent loss of data, system backup of data and system settings should be taken periodically. Backups containing PII/health data must be encrypted and access-controlled in accordance with Part VIII and Part IX of this SOP.

8. **Authentication and Access Control**

8.1 Password-based authentication and Role-Based Access Control (RBAC) to be implemented for all systems.

8.2 Passwords will be minimum 10 characters with a mix of alphanumeric and special characters; minimum 12 characters for systems processing health data.

8.3 To protect against unauthorized physical access, users will lock systems using screensaver, login, and BIOS password.

8.4 All users must shut down systems when leaving office premises.

8.5 No unauthorized user shall be permitted to access/open hardware devices.

8.6 Features like camera, Wi-Fi, voice recording, Bluetooth, GPS, and geo-tagging will be disabled on official devices.

Software Security Management

9. **Software Security**

9.1 Operating System (OS). Only licensed versions of OS will be used. Installation of dual boot/virtualized OS at user level is strictly prohibited.

9.2 Application Software. Users will only use licensed, vetted application software from authorized sources. Any health data management application must be assessed for DPDP compliance before deployment.

9.3 Software Updating. Administrators will ensure software is regularly updated with genuine patches. Security patching of health data systems is a priority and must not be deferred beyond 72 hours of patch release.

9.4 Pirated Software. Use of pirated/unlicensed/cracked software is strictly

prohibited.

9.5 System Hardening. Actions for system hardening: (i) BIOS software hardened; unauthorized peripherals disabled. (ii) Network administrators to re-configure systems, disabling all non-essential services.

10. Anti-Malware Software. A comprehensive anti-malware security suite providing anti-virus, anti-spam, and anti-rootkit features must be installed. Real-time protection must remain active on all systems processing PII or health records.

11. Personal Firewall. Firewall must be enabled on all personal computers. Inbuilt Windows Firewall must remain enabled as a minimum baseline.

12. Encryption Software. File and folder encryption software (such as Vera Crypt) shall be used for all data containing PII or health information. Encryption is mandatory for any portable media or laptop containing such data.

User Access Control

13. Access control policy ensures Role-Based Access (RBAC). Network administrators at all levels will ensure:

13.1 Privilege Management. Users must log in with user rights only. Administrator accounts managed exclusively by Network Administrators.

13.2 Password Management. Users will implement multilevel password-based authentication including BIOS password, user account login, and screensaver password.

13.3 Management of USB Ports. USB Ports disabled on all computers to prevent unauthorized data transfer.

13.4 Data Ownership. User remains sole owner/custodian of data on their computer and is responsible for all terminal end-user level violations.

13.5 Health Data Access Logging. All access to systems containing health records must be logged with user ID, timestamp, and action performed. Logs must be retained as running logs for a minimum of 2 years on accessible storage, followed by archival for a minimum of 5 years, in accordance with DPDP Act 2023 obligations and the ECHS Log Retention Policy (refer Part VI, para 35A).

14. Security of System Documentation. System documents/files (including logs, configuration files, photocopiers, MFDs etc.) must be stored on designated computers securely to prevent unauthorized access, modification or deletion.

15. Unauthorized Data. Unauthorized data like personal documents, presentations, multimedia files, pornographic content etc. will not be stored within official systems.

PART II: INTRA-NETWORK SECURITY

Network Management

16. Responsibility of Network Management. Networks will be managed and controlled to protect them from cyber threats. Appropriate security solutions will be incorporated at physical, network, transport and application layers. Network segments handling health data and PII must be isolated from general-purpose network segments.

Network and Application Access Control

17. Access to both internal and external network services/resources will be as follows:

17.1 Remote Access Software. Third party applications for remote access (e.g., TeamViewer, VNC) are prohibited on official computers.

17.2 Access Control. Access to software and related information will be restricted to authorised users only. RBAC matrices for health data systems must be documented and reviewed quarterly.

17.3 Security of Application Software. The classification of application software will be explicitly defined and documented. Health data applications must be assessed for DPDP compliance by a qualified authority.

17.4 Network Segregation for Health Data. Systems processing health records, laboratory data, or diagnostic information shall be placed on a dedicated VLAN or network segment. Cross-segment access must be logged and justified.

PART III: INTERNET SECURITY

Extension of Internet

18. Hiring of internet connectivity will be ensured primarily from Government-affiliated ISPs. Extension and securing of internet connectivity:

18.1 All internet-connected computers in office premises must have a standardized genuine OS and office software along with requisite cyber security controls. Wi-Fi adaptors within official devices must be disabled.

18.2 A list of users authorized internet connectivity within the office premises must be maintained.

18.3 No Health Data on Internet Computers. Systems connected to the internet must not store or process health records, PII, or beneficiary data unless protected by end-to-end encryption approved by the Data Protection Officer (DPO).

19. Internet computers will not be connected to:

19.1 Mobile phones.

19.2 'Plug and Surf' type GSM/CDMA USB modems.

19.3 Wi-Fi/Bluetooth/NFC adaptors, dongles, etc.

20. Zero Tolerance for Use of Pen Drives and Air Gap Violations. The use of pen drives is strictly prohibited. Air gap violations will invite strict administrative proceedings. No personal data will be processed or stored on internet PCs.

Prevention of Data Leakage

21. Data leakage may take place inadvertently or by use of unauthorized software. Controls include:

21.1 Computer or user account names configured on internet computers must not reveal appointment/identity of person/unit using the computer.

21.2 Unauthorized software (e.g., Messenger/chat software, File Sharing software, Remote Access software) will not be installed on official computers.

21.3 Health Data Leakage Prevention (DLP). Data Loss Prevention (DLP) tools must be configured on all systems processing health data. Any attempt to email, upload, or transfer unencrypted PII/health data must be blocked and flagged.

PART IV: ASSET MANAGEMENT AND DATA HANDLING

22. Inventory of Assets. Inventory of cyber/IT assets and infrastructure must be prepared and updated periodically. A separate register identifying all systems containing PII or health data must be maintained and reviewed at every cyber security audit (Refer Annexure D).

23. Ownership and Accountability of Assets. All cyber/IT assets will be held on charge of a designated holder or user. Theft/loss must be reported promptly. Any loss of assets containing health data or PII must also be reported to the Data Protection Officer (DPO) within 24 hours as a potential data breach under DPDP Act 2023.

24. Accounting of Secondary Mass Storage Devices. Strict control to be exercised in use of secondary mass storage devices such as CD/DVD writers and NAS drives. All such devices storing health data must be encrypted.

25. Equipment Maintenance and Repair. Faulty hard disks will be destroyed in-situ by an authorized Board of Officers. Under no circumstances will hard disks containing beneficiary data be returned to the vendor.

26. Disposal of Storage Media/Printer Cartridges. Storage media and used printer cartridges will be securely destroyed through disintegration, incineration, melting, or shredding. Any media containing health data or PII must be securely erased (minimum 3-pass DoD wipe) before physical destruction. A Board of Officers record of all such destruction must be maintained for audit.

Handling of Removable Storage Media

27. Ban on USB-Based Storage Media. Use of removable USB-based storage devices is banned. All types of memory sticks, external USB drives, SD cards, MMC cards, PDAs, and mobile phones come under this ban.

Unauthorized Possession of Information/Data

28. Handing/Taking Over by All Ranks. All ranks/personnel will ensure that no official data, particularly health records or PII of beneficiaries, is retained on personal IT assets. The Handing/Taking over Certificate will include the following declaration:

28.1 I am not carrying soft/hard copy of any classified/unauthorized information/data, including health records or personal data of ECHS beneficiaries.

28.2 I am aware that violation of the above declaration will render me liable to disciplinary action under service regulations and penalties under the DPDP Act 2023.

Change Management

29. All changes in hardware, software and their configuration will be duly analyzed and carried out in a controlled manner under supervision. The following need to be ensured:

29.1 System Formatting, Recovery, Repair and Restore. Permission from appropriate authority will be obtained prior to formatting, recovery, repair or restoration of information system assets. Systems containing health data must undergo a verified data-wipe prior to formatting.

29.2 Maintenance of Records. Records of system formatting, recovery, repair, or restoration will be maintained in designated registers and produced during internal and external cyber security audits.

30. Change of Appointment. On change of appointment, de-facto formatting of computers will not be resorted to. Access rights will be immediately revoked upon transfer. The network administrator will issue fresh user credentials with RBAC to the new incumbent.

PART V: PHYSICAL AND ENVIRONMENT SECURITY

31. Secure Areas. Information processing facilities will be housed in secure areas. Entry will be controlled, regulated, and monitored. IT assets deployed in common/unattended areas must be secured against unauthorized access.

32. Access Security. Security parameters such as access cards, biometric access devices, controlled entry points, or manned reception desks will be used to establish entry to areas containing information and information processing facilities.

33. Power Supply. IT equipment will be protected from power failures and other disruptions. UPS and backup power will be provided.

34. Network Cabling. All network cabling and test points will be protected from unauthorized interception and damage. All cables should be uniquely marked. Unused network sockets should be blocked. MAC binding must be ensured in all network switches.

PART VI: AUDITS AND INCIDENT MANAGEMENT

Audits

35. The Station HQ shall nominate suitable members to constitute audit teams. Records of audits to be maintained and furnished during Annual Inspections:

35.1 Internal Audits. Internal audits to be undertaken on quarterly basis by nominated agencies. Audit checklist must include a dedicated DPDP/PII compliance section from 2025 onwards.

35.2 External Audits. External audits to be undertaken on annual basis by nominated agencies. DPDP compliance must be independently assessed as part of the annual external audit.

35A. Log Retention Policy

System and application logs constitute critical evidence for cyber incident investigation, regulatory compliance, and forensic analysis. The following mandatory log retention standards apply to all ECHS IT assets, including workstations, servers, network devices, firewalls, anti-malware systems, health data applications, and identity management systems. All Network Administrators and OIC PCs are responsible for implementing and verifying compliance with this policy within their area of responsibility.

35A.1 Running Logs (Active / Online Retention). All system and application logs shall be maintained as running logs on accessible, queryable storage for a minimum of 2 (two) years from the date of generation. Running logs must remain readily available for real-time monitoring, incident investigation, and audit purposes without requiring restoration from archive. Log integrity must be maintained through tamper-evident controls (e.g., write-once storage, cryptographic hashing, or centralised log management with access controls). The following log types are covered as a minimum: OS event logs; authentication and access logs (login, logout, failed attempts); application logs for health data and PII-processing systems; firewall and network device logs; anti-malware and IDS/IPS alert logs; administrative action logs; patch deployment logs; and data access logs for CONFIDENTIAL and above information.

35A.2 Archival Logs (Offline / Cold Storage Retention). Upon completion of the 2-year running period, all logs shall be transferred to offline or cold storage (e.g., encrypted tape, optical media, or dedicated archival system) and retained for a minimum of 5 (five) years. Archived logs must be retrievable within 72 hours upon request from an authorised officer, the DPO, or a regulatory authority. The integrity of archived logs shall be verified at the point of archival and upon retrieval. Archived logs shall be stored in encrypted form (AES-256 or equivalent) and protected against unauthorised access, modification, or premature deletion. A Custody and Integrity Record must be maintained for all archived log sets, recording: log type, date range, archival date, storage medium/location, and responsible officer.

35A.3 Legal Hold. Where logs are material to an ongoing cyber incident investigation, regulatory inquiry, litigation, or disciplinary proceeding, a legal hold shall be applied. Logs under legal hold shall not be deleted or overwritten regardless of the expiry of the standard retention period. The legal hold shall be lifted only upon written authorisation of the DPO or Legal/Compliance Officer. The retention period for such logs extends until the matter is fully

resolved and the hold formally lifted.

35A.4 Disposal. On expiry of the 5-year archival period (or any extended legal hold period), logs shall be securely deleted using approved data sanitisation methods (minimum 3-pass DoD wipe for digital media; physical destruction for tape/optical media). Disposal shall be recorded in the Asset and Log Disposal Register maintained by the Network Administrator at each PC/RC. No logs shall be deleted prior to the expiry of the applicable retention period without written authorisation from CO ECHS.

35A.5 Compliance and Audit. Compliance with this Log Retention Policy shall be verified at every quarterly cyber security audit (para 35). The DPO shall include log retention compliance status in the quarterly metrics report to CO ECHS (para 61). Non-compliance — including premature deletion, failure to archive, or inaccessible archived logs — shall be treated as a cyber-violation under this SOP and may attract disciplinary action.

Incident Reporting and Handling

36. Cyber Incidents. Cyber incident is an adverse event on a computer/information system/network or a threat of occurrence. Examples include loss of information, compromise of access controls, or malware infection. Any incident involving health data or PII additionally constitutes a Personal Data Breach under the DPDP Act 2023.

37. Incident Reporting. All cyber security incidents will be reported to CERT-Army through respective IW/GS Staff at various levels (Stn HQ/Sub Area HQ/Area HQ/Corps HQ/Comd HQ) with a copy to CO ECHS. Personal data breaches must additionally be reported to the Data Protection Officer (DPO) within 6 hours and to the Data Protection Board of India (DPBI) within 72 hours as mandated by the DPDP Act 2023. Refer Annexure C for Data Breach Response Protocol.

PART VII: DIGITAL PERSONAL DATA PROTECTION (DPDP) ACT 2023 COMPLIANCE (NEW SECTION — Mandatory from Financial Year 2025-26)

IMPORTANT — Legal Obligation
The Digital Personal Data Protection (DPDP) Act 2023 is a Central Act of India and its provisions are legally binding on ECHS as a Data Fiduciary. Non-compliance may result in penalties up to ₹250 crore per breach instance as imposed by the Data Protection Board of India. All Officers must familiarize themselves with their obligations under this Act.

38. Overview of the DPDP Act 2023

The Digital Personal Data Protection (DPDP) Act 2023 (No. 22 of 2023) was enacted by the Parliament of India and governs the processing of digital personal data of Indian citizens. As ECHS processes health data and other sensitive PII of a large number of beneficiaries — including retired defense personnel, their dependents, and children — it falls squarely under the obligations of this Act.

39. Key Definitions under DPDP Act 2023

Term	Definition (as applicable to ECHS)
Personal Data	Any data about an individual who is identifiable by or in relation to that data. In ECHS context: Name, Service Number, Aadhaar Number, date of birth, address, contact details of beneficiaries.
Data Fiduciary	The entity that determines the purpose and means of processing personal data. ECHS is a Data Fiduciary for its beneficiary database.
Data Principal	The individual whose personal data is being processed. For ECHS: the beneficiary (ex-serviceman, spouse, dependent, or minor child).
Data Processor	Any entity that processes personal data on behalf of the Data Fiduciary. Includes empaneled hospitals, software vendors, and IT service providers of ECHS.
Significant Data Fiduciary (SDF)	A Data Fiduciary notified by Central Government based on volume/sensitivity of data. ECHS may qualify as SDF given the scale and sensitivity of health data processed.
Consent	A free, specific, informed, unconditional, and unambiguous indication of agreement to processing of personal data.
Personal Data Breach	Any unauthorized processing, accidental disclosure, sharing, alteration, destruction, or loss of personal data that is likely to cause harm.
Child	Any individual below the age of 18 years. All beneficiaries below 18 years of ECHS must be treated as 'children' under the Act.

40. Obligations of ECHS as a Data Fiduciary

ECHS, as a Data Fiduciary, must comply with the following obligations under the DPDP Act 2023:

40.1 Lawful Basis and Consent. ECHS must process personal data only for lawful purposes. Consent must be obtained from each beneficiary or their lawful guardian (in case of minors) before processing their personal data. Consent must be recorded in writing or electronically and must be withdrawable at any time. Refer Annexures A and B for consent form templates.

40.2 Notice before Consent. Before seeking consent, a clear and plain-language Notice must be provided to the Data Principal (beneficiary) describing: (i) what personal data will be collected; (ii) the purpose of collection; (iii) the manner in which consent may be withdrawn; (iv) how to exercise data rights; and (v) how to file a complaint with the Data Protection Board.

40.3 Purpose Limitation. Personal data of beneficiaries must be used solely for the purpose for which it was collected (e.g., provision of healthcare services). Using beneficiary data for any other purpose without explicit consent is prohibited.

40.4 Data Minimization. ECHS must collect only the minimum personal data necessary for the specified purpose. Collection of excessive or unrelated personal information is prohibited.

40.5 Data Accuracy. Reasonable steps must be taken to ensure that personal data is accurate, complete, and updated, particularly where the data is used to make decisions affecting the Data Principal.

40.6 Storage Limitation. Personal data must not be retained beyond the period necessary for the stated purpose. A Data Retention Schedule (see para 48) must be maintained and followed.

40.7 Data Security. ECHS must implement reasonable security safeguards to prevent personal data breaches. This includes technical, administrative, and physical safeguards as detailed in this SOP.

40.8 Grievance Redressal. ECHS must establish a Data Principal Grievance Redressal mechanism. The Data Protection Officer (DPO) will serve as the nodal point for grievance resolution within 30 days of receipt.

40.9 Data Processor Contracts. ECHS must ensure that all Data Processors (empaneled hospitals, IT vendors, software providers) sign a written Data Processing Agreement (DPA) containing terms consistent with DPDP Act obligations. Data Processors must not process data beyond the instructions of ECHS.

40.10 Breach Notification. In case of a personal data breach, ECHS must notify the Data Protection Board of India and the affected Data Principals as prescribed. Refer para 37 and Annexure C.

41. Rights of Data Principals (ECHS Beneficiaries)

Every ECHS beneficiary, as a Data Principal, has the following rights under the DPDP Act 2023. ECHS must have procedures in place to honor these rights:

41.1 Right to Information. The beneficiary has the right to obtain a summary of their personal data processed by ECHS and the processing activities undertaken.

41.2 Right to Correction and Erasure. The beneficiary has the right to correct inaccurate or misleading personal data, to complete incomplete data, and to request erasure of personal data no longer necessary for the processing purpose.

41.3 Right to Grievance Redressal. The beneficiary has the right to have their grievances related to data processing addressed by the DPO and thereafter to approach the Data Protection Board of India.

41.4 Right to Nominate. The beneficiary has the right to nominate another individual who shall exercise their rights in the event of death or incapacity.

41.5 Right to Withdraw Consent. The beneficiary has the right to withdraw consent at any time. Withdrawal shall not affect the lawfulness of processing prior to withdrawal. ECHS must cease processing upon withdrawal unless there is another lawful basis.

Grievance Redressal Contact
All Data Principal grievances must be addressed to the Data Protection Officer (DPO), CO ECHS, Delhi Cantt-10. Grievances must be acknowledged within 48 hours and resolved within 30 days.

42. Appointment and Role of Data Protection Officer (DPO)

A Data Protection Officer (DPO) shall be designated at CO ECHS level. The DPO shall:

42.1 Be a senior officer of appropriate rank with knowledge of data protection law and ECHS's IT infrastructure.

42.2 Serve as the single point of contact for all DPDP Act compliance matters.

42.3 Liaise with the Data Protection Board of India (DPBI) on behalf of ECHS.

42.4 Receive and redress Data Principal grievances within prescribed timelines.

42.5 Oversee Data Protection Impact Assessments (DPIAs) for new IT systems processing health data.

42.6 Conduct or oversee annual DPDP compliance audits.

42.7 Maintain the Register of Processing Activities (ROPA) for ECHS.

42.8 Coordinate breach notification to DPBI and affected Data Principals.

43. Data Retention Schedule

Personal data must not be retained beyond what is necessary. The following schedule applies to ECHS beneficiary data:

Data Category	Retention Period	Disposal Method
Active beneficiary health records	Duration of enrolment + 7 years	Secure deletion; Board of Officers record
Deceased beneficiary records	10 years from date of death	Secure deletion with audit trail
Minor beneficiary records	Until age 25 or 7 years post last treatment, whichever is later	Secure deletion; parental/guardian consent for closure
Access logs and audit trails	2 years running; minimum 5 years archival	Running logs: accessible online storage for 2 years; archived to offline/cold storage thereafter; secure deletion after 5-year archival period
Consent records	Duration of processing + 3 years	Archived with DPO; secure deletion after period
Data breach records	Minimum 5 years	Archived with DPO; legal hold if under litigation
IT system logs	2 years running; minimum 5 years archival	Running logs on accessible storage for 2 years; archived to offline/cold storage for 5 years; secure deletion thereafter with audit record

44. Third Party / Data Processor Obligations

ECHS engages third parties including empaneled hospitals, diagnostic labs, IT system vendors, and cloud service providers. All such entities must comply with the following:

44.1 A formal Data Processing Agreement (DPA) must be executed before any personal data is shared with a third party.

44.2 The DPA must specify: purpose limitations, data security requirements, sub-processor restrictions, breach notification timelines, data return/deletion obligations, and audit rights.

44.3 Empaneled hospitals receiving beneficiary health data must be assessed for their own DPDP compliance annually.

44.4 No personal data of ECHS beneficiaries may be transferred outside India unless

compliant with Section 16 of the DPDP Act 2023 (cross-border data transfer provisions).

44.5 Third-party systems accessing ECHS data must undergo a security assessment before integration.

PART VIII: PERSONALLY IDENTIFIABLE INFORMATION (PII) AND HEALTH DATA PROTECTION
(NEW SECTION — Mandatory from Financial Year 2025-26)

Health Data — Highest Sensitivity
Health data is one of the most sensitive categories of personal data. Under the DPDP Act 2023 and the EHR Standards 2023, health data of ECHS beneficiaries carries the highest level of protection obligation. Any compromise of health data may cause significant harm to the beneficiary including discrimination, stigma, and financial loss. All personnel handling health data must treat it with the utmost care.

45. Classification of PII in ECHS

The following categories of personal data are processed by ECHS and must be protected accordingly:

Level	Data Category	Examples
CRITICAL	Health & Medical Data	Diagnosis, treatment records, prescriptions, lab reports, surgical history, mental health records, HIV/AIDS status, disability details
CRITICAL	Biometric & Identity Data	Aadhaar number, fingerprints, iris scans, photograph, Service Number
HIGH	Financial PII	Bank account details, pension details, insurance numbers
HIGH	Contact & Demographic PII	Name, date of birth, address, phone number, email, family member details
MEDIUM	Service Records	Rank, unit, service period, discharge details
MEDIUM	Administrative Data	ECHS card number, registration date, appointment history

46. Technical Safeguards for Health Data

The following mandatory technical controls apply to all systems processing health data or PII of ECHS beneficiaries:

46.1 Encryption at Rest. All health data stored in databases, files, or backup media must be encrypted using AES-256 or equivalent. Unencrypted health data must not reside on any portable device.

46.2 Encryption in Transit. All transmission of health data over any network (including internal ECHS network) must be encrypted using TLS 1.2 or higher. Transmission of PII via unencrypted email is prohibited.

46.3 Access Control and RBAC. Access to health data systems must be strictly role-based. Only personnel with a clinical or administrative need-to-know may access individual beneficiary records. Role matrices must be documented and reviewed quarterly.

46.4 Audit Logging. All access to, modification of, or deletion of health records must be automatically logged. Logs must include user ID, timestamp, record accessed, and action performed. Logs must be tamper-proof and retained as running logs for a minimum of 2 years on accessible storage, followed by archival for a minimum of 5 years, in accordance with the ECHS Log Retention Policy (refer Part VI, para 35A).

46.5 Data Masking/Anonymization. For training, testing, or statistical purposes, health data must be anonymized or pseudonymised. Real beneficiary data must not be used in non-production environments.

46.6 Database Security. Health data databases must be hosted on isolated servers. Database admin accounts must be separate from application accounts. Database activity monitoring must be enabled.

46.7 Multi-Factor Authentication (MFA). All personnel accessing health data systems must authenticate using a minimum of two factors (e.g., password + OTP or biometric). MFA is mandatory for remote access to health data.

46.8 Session Management. Health data application sessions must automatically timeout after 5 minutes of inactivity. Session tokens must be invalidated on logout.

47. Administrative Safeguards for Health Data

(a) Data Protection Impact Assessment (DPIA). Before deploying any new system that will process health data, a DPIA must be conducted by the DPO. The DPIA must assess risks to beneficiary privacy and document mitigation measures.

(b) Need-to-Know Principle. Health data must be accessible only to personnel who require it for their official duties. Display or discussion of beneficiary health data in open areas is prohibited.

(c) Training and Awareness. All personnel handling health data must complete mandatory annual training on DPDP Act obligations, health data security, and incident reporting procedures. Training records must be maintained by the DPO.

(d) Confidentiality Undertaking. All personnel with access to health data must sign a Confidentiality Undertaking (Oath of Secrecy covering personal data) at the time of joining and annually thereafter.

(e) De-identification before Sharing. Before sharing health data for any analytical, reporting, or research purpose, data must be de-identified such that individual beneficiaries cannot be re-identified.

(f) Physical Security of Health Records. Physical health records (if maintained) must be stored in locked cabinets accessible only to authorized personnel. Physical records must not be removed from premises without written authorization.

(g) Screen Privacy. Personnel accessing beneficiary health data on screens must use privacy screens in areas accessible to the public or other personnel. Screens must be locked or turned away from public view.

48. Health Data Sharing Protocol

Health data of ECHS beneficiaries may only be shared in the following circumstances and with the following controls:

(a) With Empaneled Hospitals. Only the data necessary for treatment (minimum necessary principle). Sharing must be covered by the Data Processing Agreement. Sharing must be encrypted.

(b) With Government Agencies. Only pursuant to a lawful order, statutory provision, or court direction. The DPO must be informed before sharing. Only aggregated/de-identified data to be shared for policy/statistical purposes unless individual data is specifically required.

(c) With Family Members. Health data of a beneficiary may only be shared with family members with the explicit consent of the beneficiary, or in cases of medical emergency, or in case of minors as per Part IX of this SOP.

(d) Prohibited Sharing. Health data of beneficiaries must not be shared with: insurance companies without explicit consent; pharmaceutical companies; employers; media; or any entity not having a lawful basis for receiving it.

(e) Record of Sharing. Every instance of data sharing must be recorded in a Data Sharing Register maintained by the DPO, documenting: recipient, data shared, purpose, legal basis, and date.

PART IX: PROTECTION OF CHILDREN'S PERSONAL DATA (MINOR BENEFICIARIES) (NEW SECTION — Mandatory from Financial Year 2025-26)

CRITICAL — Special Protection for Minor Beneficiaries
The DPDP Act 2023 accords the highest level of protection to the personal data of children (persons below 18 years). Section 9 of the DPDP Act 2023 mandates that a Data Fiduciary must obtain verifiable parental or guardian consent before processing any personal data of a child. ECHS must strictly comply with these provisions for all minor dependant beneficiaries.

49. Identification of Minor Beneficiaries

For the purpose of this SOP, a minor beneficiary is any ECHS-enrolled dependent who is below 18 years of age. ECHS must:

- Maintain a separate, clearly tagged register of all minor beneficiaries enrolled.
- Ensure that the ECHS Health Management Information System (HMIS) flags all records belonging to beneficiaries below 18 years of age.
- Review and update the minor status of beneficiaries on their 18th birthday and transition their data protection treatment to adult provisions accordingly.
- Not rely on self-reporting for age. Age must be verified through valid government documents (birth certificate, school leaving certificate, Aadhaar) before enrolment.

50. Parental/Guardian Consent for Minor Beneficiaries

The following requirements apply to all processing of personal data of minor beneficiaries:

(a) Verifiable Parental/Guardian Consent. Before collecting or processing any personal data of a minor beneficiary, ECHS must obtain verifiable consent from the parent or lawful guardian. Consent must be in writing (physical or electronic) and must be documented (Refer Annexure B for the consent form template).

(b) Consent at Enrolment. Parental/guardian consent must be obtained at the time of enrolment of a minor beneficiary and must cover all routine health data processing activities.

(c) Separate Consent for Sensitive Procedures. For sensitive medical procedures, mental health consultations, reproductive health services, or any non-routine health data processing involving a minor, separate additional consent must be obtained from the parent/guardian and documented.

(d) Consent of the Minor. Where the minor beneficiary is 14 years or above, their assent (in addition to parental/guardian consent) should be documented as a best practice, particularly for sensitive health data.

(e) Withdrawal of Consent. Parents/guardians may withdraw consent at any time. Upon withdrawal, ECHS must cease processing of the minor's personal data for the affected

purpose and delete the data if no other lawful basis exists.

(f) Change in Guardianship. In case of change in guardianship (e.g., death of parent), fresh consent must be obtained from the new lawful guardian before continuing to process the minor's data.

51. Special Restrictions for Minor Health Data

The following special restrictions apply to health data of minor beneficiaries over and above the general health data protections in Part VIII:

(a) No Profiling of Children. ECHS must not process the personal data of a child for any purpose of profiling, tracking, behavioural monitoring, or targeted advertising. Use of children's health data for any analytics beyond direct care is prohibited.

(b) Restricted Access. Access to health records of minor beneficiaries must be restricted to: treating physician/paramedic, parent/lawful guardian (upon request), and administrative staff on a strict need-to-know basis. No access without role-based authorisation.

(c) No Disclosure to Non-Guardians. Health data of a minor must not be disclosed to any person other than the treating medical team, the parent/lawful guardian, or on direction of a competent court. It must not be disclosed to other family members without parental consent.

(d) Enhanced Breach Notification. Any breach involving the personal data of a minor must be treated as a high-priority incident. In addition to standard breach notification (para 37 and Annexure C), the parent/guardian of the affected minor must be individually notified without delay.

(e) Age-Appropriate Design. Any digital interface through which minor beneficiaries or their parents/guardians provide data or access health information must be designed to be clear, plain-language, and age-appropriate.

(f) Retention of Minor Data. Health data of minor beneficiaries must be retained in accordance with the Data Retention Schedule in para 43. On reaching adulthood (18 years), the beneficiary must be provided an opportunity to review, correct, or exercise their rights over historical data.

52. Transition to Adult Data Protection

When a minor beneficiary turns 18 years of age:

- The HMIS system must automatically transition their record from 'minor' to 'adult' classification.
- The now-adult beneficiary must be sent a fresh Notice (as per para 40(b)) describing how their data has been and will be processed.
- Fresh consent must be obtained from the now-adult beneficiary in their own right (parental consent ceases to be valid).

- The beneficiary must be informed of all their rights as a Data Principal under the DPDP Act 2023.
- Any parental/guardian access that was previously granted must be revoked unless the adult beneficiary explicitly consents to continued shared access.

PART X: CYBER INCIDENT MANAGEMENT AND REPORTING PROCEDURE (NEW SECTION — Mandatory from Financial Year 2025-26)

Purpose

This Part establishes a structured, end-to-end Cyber Incident Management and Reporting Procedure for all cyber security incidents and personal data breaches at ECHS. It defines incident categories, detection and escalation protocols, Incident Response Team roles, response timelines, regulatory reporting, communication protocols, and post-incident review requirements. All ECHS personnel must be familiar with this procedure.

53. Scope and Applicability

This Incident Management Procedure applies to:

- All cyber security incidents affecting IT assets, networks, systems, or data of ECHS.
- All personal data breaches (including health data breaches) involving beneficiary PII under the DPDP Act 2023.
- Physical security incidents that may affect IT or data security (e.g., theft of a laptop or server).
- All personnel of CO ECHS, Regional Centres (RCs), Polyclinics (PCs), empanelled hospitals, and IT service providers acting on behalf of ECHS.

54. Incident Classification

All incidents shall be classified at the time of detection into one of the following severity levels. Classification drives the response timeline and escalation path:

Severity	Colour	Examples (ECHS context)	Initial Response
CRITICAL (P1)	**RED**	Ransomware on health data server; mass exfiltration of beneficiary records; compromise of Aadhaar/biometric data; breach of minor beneficiary data; loss of server/device with unencrypted PII	**Immediate ≤ 1 hour**
HIGH (P2)	**ORANGE**	Malware on health system; unauthorised access to beneficiary records; admin credential compromise; loss of encrypted device with PII; insider data theft suspected	**≤ 4 hours**
MEDIUM (P3)	**YELLOW**	Phishing email opened by staff; malware on non-critical PC; USB/air-gap violation; failed brute-force on health system; suspected (unconfirmed) data access	**≤ 24 hours**

Severity	Colour	Examples (ECHS context)	Initial Response
LOW (P4)	**GREEN**	Password policy breach; minor misconfiguration; isolated phishing not opened; suspicious activity (unconfirmed); near-miss events	**≤ 72 hours**

55. Incident Response Team (IRT)

An Incident Response Team (IRT) shall be constituted at CO ECHS, RC, and PC levels. Composition and responsibilities:

Role	Incumbent	Key Responsibilities
Incident Commander (IC)	CO ECHS / Dir RC / OIC PC	Overall authority; declares severity; authorises containment; approves all external communications
Data Protection Officer (DPO)	Designated DPO, CO ECHS	Leads data breach response; coordinates DPBI and CERT-In notification; notifies affected Data Principals; maintains breach register
Nodal Officers	Director Regional Centres	Leads data breach response; coordinates DPBI and CERT-In notification; notifies affected Data Principals; maintains breach register for Regional Centre Office and Poly Clinics in their AOR.
IT / Network Lead	Cyber Security Officer / Network Admin	Technical containment, eradication, forensic preservation, system recovery, log analysis
Legal / Compliance Officer	Dir (Stats & Automation) or nominated officer	Reviews regulatory obligations; advises on DPDP Act / IT Act; reviews reports before submission to DPBI / CERT-In
Communication Officer	PRO / Admin Officer, CO ECHS	Manages internal/external communications; drafts stakeholder notices; manages media queries through authorised channels only
Records Officer	Nominated officer at each level	Maintains incident log; documents all actions and decisions with timestamps; preserves evidence chain of custody

56. Six-Phase Incident Response Lifecycle

Every incident must pass through all six phases below. No phase may be skipped regardless of severity level:

Phase 1 — Detection and Identification

An incident may be detected through:

- Automated alerts (anti-malware, IDS/IPS, DLP, firewall, SIEM).
- Reports from ECHS staff, medical, or administrative personnel.
- Alerts from empanelled hospitals or IT service providers.
- Beneficiary complaints about unauthorised use of their data.
- Notifications from CERT-Army, CERT-In, or the Data Protection Board of India (DPBI).
- Discovery during routine audit, system maintenance, or access log review.

Upon detecting a potential incident, the detecting person must:

(a) Record the date, time, and nature of the anomaly — do not delete or modify anything.

(b) NOT attempt to investigate, remediate, or delete data without first reporting upward.

(c) Immediately inform the Network Administrator / Cyber Security Officer at the PC/RC level.

(d) Preserve all evidence in its current state; power off only if explicitly instructed by IT/Network Lead.

Phase 2 — Initial Triage and Classification

The Network Administrator/Cyber Security Officer, within 30 minutes of receiving a report, must:

(a) Assign an initial Severity Level (P1–P4) using the classification table at para 54.

(b) Activate the Incident Response Team appropriate to the severity level.

(c) Determine whether personal data (PII / health data / minor data) is likely involved — if YES, notify the DPO immediately. The DPDP Act 2023 notification clock starts from detection, not from confirmation.

(d) Open an Incident Register entry and assign a unique Incident Reference Number (IRN) in the format: ECHS/YYYYMM/[Unit Code]/[Seq]. Example: ECHS/202506/DEL01/001.

CRITICAL — DPDP Breach Clock

If personal data of beneficiaries may have been compromised, the DPO must be notified IMMEDIATELY. The 72-hour clock for DPBI notification starts from the moment of detection — not from confirmation of the breach.

Phase 3 — Containment

Containment must be initiated as quickly as possible. The IT/Network Lead executes actions appropriate to the incident type:

Incident Type	Containment Actions
Malware / Ransomware	Isolate infected system from network (disconnect LAN / disable NIC); do NOT power off (preserves memory evidence); block C2 IPs at firewall; revoke credentials of affected accounts; quarantine affected systems
Unauthorised Access / Data Breach	Revoke compromised account credentials; block attacker IP/source; isolate affected systems; preserve access logs; identify data accessed or exfiltrated; notify DPO if PII involved
Phishing Attack	Block sender domain at mail gateway; quarantine similar emails across org; reset credentials of any user who clicked; scan affected systems for malware; issue all-user advisory
Physical Theft of Device	Remotely wipe device if MDM is available; revoke all credentials on device; change all passwords potentially accessible from device; notify physical security; notify DPO if PII was on device
Insider Threat / Data Leak	Immediately revoke all access rights of suspected individual; preserve all logs; do NOT alert suspect; escalate to CO ECHS and DPO; engage Legal/Compliance Officer
USB / Air-Gap Violation	Confiscate device; forensically image media before any further use; scan system for malware; preserve chain of custody; initiate disciplinary proceedings as per service regulations and DPDP Act

All containment actions must be documented in the Incident Register with timestamps. No containment action should destroy forensic evidence without prior Incident Commander approval.

Phase 4 — Investigation and Eradication

(a) Forensic Evidence Preservation. Before remediation, create forensic images of all affected systems, storage, and logs. Preserve originals with chain-of-custody documentation. Evidence must not be altered or deleted.

(b) Root Cause Analysis (RCA). Determine: how the incident occurred; what vulnerability was exploited; what data was affected; who initiated or enabled the incident; the full timeline.

(c) Scope Determination. Identify all affected systems, accounts, and data. Specifically assess whether PII, health data, or minor beneficiary data was compromised and estimate the number of affected Data Principals.

(d) Eradication. Remove the root cause: patch vulnerabilities, remove malware, close attack vectors, fix misconfigurations. Verify eradication is complete before proceeding to recovery.

(e) Documentation. All investigation findings must be documented in detail in the Incident

Register and retained for minimum 5 years.

Phase 5 — Recovery and Restoration

- Restore systems from verified clean backups only; verify backup integrity before restoration.
- Apply all security patches before bringing systems back online.
- Reset all credentials (passwords, API keys, certificates) that may have been compromised.
- Implement enhanced monitoring on restored systems for minimum 30 days post-incident.
- Conduct a post-restoration vulnerability scan before reconnecting to the main network.
- For health data systems: verify data integrity and completeness after restoration; document any data loss for regulatory assessment.
- Obtain formal sign-off from the Incident Commander and IT/Network Lead before full operational return.

Phase 6 — Post-Incident Review (PIR)

Within 30 days of incident closure:

(a) PIR Meeting. Conduct a formal Post-Incident Review meeting covering: timeline of events; effectiveness of response; root cause and contributing factors; impact on beneficiaries; regulatory compliance during response.

(b) Lessons Learned Report. Produce a written report identifying: what worked well; what failed; corrective actions required with responsible parties and deadlines.

(c) Control Improvements. Action all identified gaps in technical, procedural, or training controls within 90 days. Report progress to CO ECHS monthly.

(d) Policy Update. If the incident reveals gaps in this SOP, the DPO must initiate a formal policy review within 30 days.

(e) Circulation of Lessons. Circulate anonymized lessons (without sensitive details) to all RC/PC officers to build organizational learning.

57. Escalation and Reporting Matrix

Timelines are from the moment of detection/discovery:

Severity	OIC PC / Dir RC	CO ECHS / DPO	CERT-Army	CERT-In (if applicable)	UIDAI (id Aadhaar Data Breach)	DPBI (if PII breach)
CRITICAL	≤ 30 min	≤ 1 hour	≤ 2 hours	≤ 6 hours	≤ 24 hours	≤ 72 hours

Severity	OIC PC / Dir RC	CO ECHS / DPO	CERT-Army	CERT-In (if applicable)	UIDAI (id Aadhaar Data Breach)	DPBI (if PII breach)
(P1)						
HIGH (P2)	≤ 2 hours	≤ 4 hours	≤ 8 hours	≤ 6 hours (if applicable)	≤ 24 hours	≤ 72 hours
MEDIUM (P3)	≤ 4 hours	≤ 24 hours	≤ 24 hours	≤ 24 hours (if applicable)	≤ 24 hours (if applicable	If PII: ≤ 72 hours
LOW (P4)	≤ 24 hours	Weekly summary	Monthly summary	If applicable	Only if Aadhaar Data Breach	Only if PII breach

58. Communication Protocols

(a) Internal Communication. Use only secure, approved channels. No incident details over personal WhatsApp, personal email, or personal mobile. A secure IRT communication channel will be established by the IT/Network Lead for all P1/P2 incidents.

(b) External Communication. No statement about an incident to any external party (media, beneficiaries, vendors, empaneled hospitals) without written authorization from the Incident Commander and CO ECHS. All external communications routed through the Communication Officer.

(c) Beneficiary Notification. Where a data breach is confirmed, affected beneficiaries must be individually notified in plain language within 7 days of confirmation, covering: what happened; what data was affected; steps ECHS is taking; what the beneficiary can do; DPO contact details. For incidents involving minor data: notify parent/guardian immediately upon confirmation.

(d) Regulatory Reporting. CERT-Army reports must follow CERT-Army prescribed format. CERT-In reports must use Annexure F of this SOP. DPBI reports must follow DPBI prescribed format. All regulatory reports must be reviewed by the DPO and Legal/Compliance Officer before submission.

(e) Media Queries. All media queries must be referred to the PRO, CO ECHS. No officer below CO ECHS level is authorized to respond to media queries about any cyber incident or data breach.

59. Incident Register

The DPO / Records Officer must maintain a centralized Incident Register at CO ECHS level. Each RC/PC maintains a local register. The register must record:

- Every incident (all severity levels) including near-misses and false positives.
- Unique IRN, date/time of detection, reporting timelines at each level, severity level.
- Incident description, systems/data affected, containment actions, resolution status.

- All regulatory notifications (CERT-Army, CERT-In, UIADI, DPBI) with dates and reference numbers.
- Status: Open / Under Investigation / Contained / Resolved / Closed.
- Reference to PIR report and lessons learned document.

The Incident Register must be produced at all internal and external audits, reviewed monthly by the DPO, and quarterly by the Incident Commander.

60. Incident Management Training and Drills

(a) Initial Training. All newly posted personnel must complete incident management training within 30 days of joining.

(b) Annual Refresher. Annual refresher training on incident management and DPDP Act obligations for all personnel with IT/health data access. Records maintained by the DPO.

(c) Tabletop Exercises. Minimum one tabletop exercise per year at RC level, and one at CO ECHS level. Scenarios must include: ransomware on health data systems; breach of minor beneficiary data; insider data theft; and physical device theft. Drill reports due to CO ECHS within 15 days.

61. Metrics Reporting to CO ECHS

Monthly metrics compiled by the DPO and reported to CO ECHS:

- Total incidents by severity and category.
- Mean Time to Detect (MTTD), Mean Time to Contain (MTTC), Mean Time to Resolve (MTTR).
- Number of PII / health data breaches; number of Data Principals affected.
- DPBI / CERT-In notifications made and outcomes.

Status of all open Post-Incident Review corrective actions.

PART XI: PASSWORD MANAGEMENT POLICY

Passwords are the primary mechanism for authenticating users to ECHS IT systems, including systems processing Personal Identifiable Information (PII), health records, and financial data. Weak or compromised passwords are a leading cause of unauthorised access and data breaches. This Part establishes mandatory password management standards for all ECHS personnel, contractors, and vendors with access to ECHS IT infrastructure.

62. Multi-Level Password Protection

Every computer system shall be protected with multi-level passwords at the BIOS, Operating System (OS), and application levels. Each authentication level shall use a distinct, independently maintained password. Users shall not reuse the same password across different levels.

63. Password Complexity Requirements

All passwords shall conform to the following complexity requirements:

- Minimum length of eight (08) characters for standard accounts; minimum twelve (12) characters for accounts accessing health data or PII (refer Part VIII, para 8.2).
- Mandatory combination of: uppercase letters (A–Z), lowercase letters (a–z), digits (0–9), and at least one special character from the set: ! @ # $ % ^ & * ( ) [ ] { } : ; “ ’ < > ? /
- Passwords must not be based on dictionary words, names, dates of birth, service numbers, or any personally identifiable information, to preclude vulnerability to dictionary attacks and social-engineering guessing.

64. Password Change and Expiry

Passwords shall be changed at least once every thirty (30) days, or immediately upon any indication or suspicion of compromise. Mandatory periodic change shall be enforced through Group Policy on all domain-joined systems. Temporary and default passwords issued at account creation shall be changed upon first logon without exception. Recycling of the last five (05) passwords is prohibited; the system shall enforce this restriction technically.

65. Password Confidentiality

Passwords are strictly personal and shall not be shared with any other individual, including supervisors, colleagues, or IT support personnel. Passwords shall not be written on chits, sticky pads, notepads, whiteboards, or any other physical medium, nor stored in unencrypted electronic files. The “Remember Password” feature of browsers and applications shall be disabled on all official systems. Any suspicious activity or unauthorised access logged against a particular User ID shall be the sole responsibility of the registered user of that account. Disclosure of passwords in any form may constitute a cyber-violation under this SOP and shall attract disciplinary action.

66. Account Lockout and Session Management

Systems shall be configured by the Network Administrator to automatically lock user accounts after three (03) consecutive failed login attempts. Unlocking of locked accounts shall require intervention by the Unit/PC IT Administrator and shall be logged. Lock screen shall activate automatically if the system remains idle for five (05) minutes or more. This setting shall be enforced via Group Policy and shall not be overridden at the user level.

67. Encryption of Authentication Credentials

Authentication credentials, including passwords, shall be encrypted both in storage (using

accepted hashing algorithms, e.g., bcrypt, SHA-256) and in transit (using TLS 1.2 or above). Applications and systems shall never store passwords in plain text. Passwords shall not be visible on-screen during entry; masked input is mandatory for all authentication interfaces deployed on ECHS systems.

68. Responsibility and Enforcement

Compliance with this Password Management Policy is mandatory for all ECHS personnel, attached staff, and vendors with system access. Network Administrators at each PC/RC shall configure and audit Group Policy settings to ensure technical enforcement of complexity, expiry, lockout, and screen-lock requirements. Non-compliance shall be treated as a cyber-violation under this SOP and may attract disciplinary action. Passwords classified as compromised shall be reported as a LOW (P4) security incident per Part X, para 54, and remediated immediately. The DPO shall include password policy audit results in the quarterly security metrics report to CO ECHS (para 61).

PART XII: PATCH MANAGEMENT POLICY

Unpatched software and firmware are among the most frequently exploited attack vectors in cyber incidents. This Part establishes mandatory requirements for the timely identification, testing, and application of security patches and updates across all ECHS IT assets, including end-user workstations, servers, network devices, and operating systems. These requirements apply to all ECHS personnel and Network Administrators at every PC, RC, and CO ECHS.

69. Patch Classification and Priority

All patches and updates shall be classified by the Network Administrator according to the following priority levels before deployment:

- **Critical** — Patches addressing actively exploited vulnerabilities or those rated Critical by the vendor (CVSS score ≥ 9.0). Mandatory deployment within 72 hours of release on all affected ECHS systems. Systems processing health data or PII take absolute priority (refer Part VIII, para 9.3).
- **High** — Patches rated High by the vendor (CVSS score 7.0–8.9). Deployment within 07 days of release.
- **Medium / Low** — All remaining patches. Deployment within 30 days of release as part of the regular monthly patching cycle.

70. Patch Identification and Monitoring

Network Administrators shall actively monitor vendor security advisories, CERT-In alerts, and CERT-Army bulletins for newly released patches affecting ECHS IT assets. An up-to-date asset inventory (refer Part IV, para 22) shall be maintained to enable rapid identification of all systems requiring a given patch. Any unpatched system shall be flagged and tracked until the patch is applied or an approved exception is documented.

71. Testing Before Deployment

Where operationally feasible, patches rated High or Medium/Low shall be tested on a non-production or representative system before broad deployment, to verify compatibility with existing ECHS applications and configurations. Critical patches may be deployed directly to production where immediate remediation outweighs testing risk; the Network Administrator shall document this decision. Testing shall not be used as justification for deferring Critical patches beyond the 72-hour deployment window.

72. Authorisation and Deployment

Patch deployment shall be authorised by the OIC PC or Network Administrator before execution. Only patches obtained from official vendor sources or verified repositories (e.g., Microsoft Windows Update, manufacturer portals) shall be applied; patches from unverified or third-party sources are prohibited. Automatic update features may be enabled for OS and anti-malware software provided automatic updates are limited to genuine vendor channels. All patch deployments shall be logged with date, system name, patch identifier, and name of the administrator who applied the patch. Patch deployment logs shall be retained as running logs for a minimum of 2 years and archived for a minimum of 5 years in accordance with the ECHS Log Retention Policy (refer Part VI, para 35A).

73. Rollback Procedure

A verified system backup (refer Part I, para 7.3) shall be taken before applying any patch to a critical system or server. If a patch causes system instability, application failure, or data

inconsistency, the Network Administrator shall immediately initiate rollback using the pre-patch backup and report the incident to OIC PC. The rollback event shall be logged and reported to CO ECHS. A deferred re-patching plan shall be prepared and implemented within 14 days of rollback.

74. Exceptions and Compensating Controls

Where a patch cannot be applied within the prescribed timeline due to operational constraints or compatibility issues, the Network Administrator shall submit a documented exception request to the OIC PC, stating the reason for deferral, the affected systems, and proposed compensating controls (e.g., enhanced monitoring, network isolation, restricted access). All approved exceptions shall be reviewed at the next quarterly cyber security audit. No exception shall be granted for Critical patches on systems processing health data or PII without written approval from CO ECHS.

75. Audit and Compliance

Network Administrators shall maintain a Patch Register recording all patches identified, their priority classification, target systems, deployment date, and outcome. This register shall be produced at every quarterly cyber security audit (refer Part VI, para 35). The Patch Register and associated deployment logs shall be retained as running records for a minimum of 2 years and archived for a minimum of 5 years in accordance with the ECHS Log Retention Policy (refer Part VI, para 35A). Patch compliance status shall be included in the metrics report to CO ECHS (para 61). Failure to apply patches within prescribed timelines without an approved exception shall be treated as a cyber-violation under this SOP and may attract disciplinary action.

PART XIII: INFORMATION CLASSIFICATION POLICY

ECHS, as a Data Fiduciary under the Digital Personal Data Protection (DPDP) Act 2023 and an organisation processing health and identity data of defence personnel, generates and handles information of varying sensitivity. Failure to classify information appropriately leads to inadequate protective controls, over-sharing, regulatory non-compliance, and security breaches. This Part establishes a mandatory Information Classification Policy covering generic government information categories and special-category data including Aadhaar, Personally Identifiable Information (PII), and Health Records, with reference to the DPDP Act 2023, the Information Technology Act 2000, and the Classification and Handling of Classified Documents — 2001. All ECHS personnel, contractors, and vendors handling ECHS information shall comply with this Policy.

76. Scope and Applicability

This Policy applies to all information created, received, stored, processed, or transmitted by ECHS in any form — physical or electronic — including documents, records, databases, emails, printouts, and portable media. It covers all ECHS IT assets identified in the Asset Register (refer Part IV, para 22) and all personnel with access to ECHS information assets.

77. Generic Classification Tiers

All ECHS information shall be assigned one of the following four generic classification tiers at the point of creation or receipt. The classification shall be reviewed whenever the information is substantially modified, transferred, or prepared for disposal.

- **TOP SECRET / SECRET** — Information whose unauthorised disclosure would cause exceptionally grave or serious damage to national security or to the functioning of the defence establishment. Governed by Classification and Handling of Classified Documents — 2001. Access on strict need-to-know basis only.
- **CONFIDENTIAL** — Information whose unauthorised disclosure could damage ECHS operations, compromise beneficiary welfare, or constitute a regulatory breach. Includes personal data of beneficiaries, internal audit reports, vendor contracts, and system architecture documents. Access restricted to authorised personnel with a defined role-based need.
- **RESTRICTED** — Internal working information not intended for public release, but whose disclosure would cause limited harm. Includes internal circulars, administrative correspondence, non-sensitive operational data, and meeting minutes. Access limited to ECHS personnel on a need-to-know basis.
- **UNCLASSIFIED / PUBLIC** — Information approved for public release or with no foreseeable harm from disclosure. Includes publicly issued notifications, approved press releases, and publicly available scheme guidelines. No special handling controls required beyond basic accuracy checks before release.

78. Special Category Data — Aadhaar, PII, and Health Records

Certain categories of data processed by ECHS carry heightened legal obligations and attract additional protective controls beyond the generic classification tiers above. These are mandatorily classified as CONFIDENTIAL as a minimum and are subject to the following specific statutory frameworks:

- **Aadhaar Data** — Includes Aadhaar numbers, biometric data, demographic data, and authentication records linked to an Aadhaar identity. Governed by the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016 and UIDAI Regulations. Aadhaar numbers shall be stored only in masked or tokenised form (last four digits visible only). Collection is limited to the purpose of beneficiary identity verification as permitted by law. Sharing of Aadhaar data with third parties is strictly prohibited except as required by law. Any breach shall be reported per the Aadhaar Data Breach Reporting Form (Annexure H, where applicable) and the DPDP Act 2023 breach protocol (para 37).
- **Personally Identifiable Information (PII)** — Includes name, date of birth, service number, contact details, financial data, and any other data that can individually or in combination identify a beneficiary or their dependants. Governed by the DPDP Act 2023 ("Personal Data" as defined under Section 2(t)) and the IT Act 2000 (Section 43A — reasonable security practices for sensitive personal data). Collection shall be limited to the minimum necessary for the defined ECHS purpose (data minimisation). PII shall be processed only for the lawful purpose for which consent was obtained (refer Annexures A and B). It shall not be retained beyond the period specified in the ECHS Data Retention Schedule (refer Part VII, para 40.8) and must be securely deleted or anonymised upon expiry.
- **Health Records / Medical Data** — Includes diagnosis records, prescription data, laboratory results, radiology reports, treatment histories, disability certificates, and any data that reveals the physical or mental health status of a beneficiary. Classified as CONFIDENTIAL and additionally governed by MoHFW Electronic Health Records (EHR) Standards 2023 and the DPDP Act 2023 (health data is "sensitive personal data" attracting heightened obligations). Access is restricted to authorised medical and administrative personnel with a defined clinical or administrative need (RBAC — refer Part I, para 13). Health data shall not be disclosed to any third party, insurer, employer, or family member without the explicit written consent of the beneficiary (refer Part VIII, para 46, sub-para (c)), except in a medical emergency or as required by law. Minimum password length of 12 characters applies to all systems storing health data (refer Part XI, para 63).

79. Information Classification Matrix

The following matrix summarises the key controls applicable to each information category. All controls are cumulative — higher-tier classifications inherit lower-tier controls in addition to their own.

Information Category	Minimum Classification	Legal / Regulatory Basis	Storage / Transmission	Disposal / Retention
Top Secret / Secret	Top Secret / Secret	Classification & Handling of Classified Documents — 2001; Official Secrets Act 1923	Encrypted storage on air-gapped / designated systems only; no transmission over public networks	Physical destruction per Classified Documents policy; no digital deletion without authorisation

Information Category	Minimum Classification	Legal / Regulatory Basis	Storage / Transmission	Disposal / Retention
Aadhaar Data	CONFIDENTIAL (Minimum)	Aadhaar Act 2016; UIDAI Regulations; IT Act 2000 S.43A; DPDP Act 2023	Masked / tokenised storage only; TLS 1.2+ for transmission; no storage on portable media without encryption	Secure deletion / degaussing per ECHS Retention Schedule; ADBRF required for breaches
PII (General)	CONFIDENTIAL (Minimum)	DPDP Act 2023 S.2(t); IT Act 2000 S.43A & S.72A; DPDP Rules 2025	Encrypted storage; TLS 1.2+ for transmission; RBAC access control; no unencrypted portable media	Per ECHS Retention Schedule (para 40.8); secure deletion or anonymisation on expiry
Health Records / Medical Data	CONFIDENTIAL (Heightened)	DPDP Act 2023; MoHFW EHR Standards 2023; IT Act 2000 S.43A; DPDP Rules 2025	Dedicated VLAN / isolated network segment (para 17.4); MFA mandatory (para 46.7); 12-char password minimum; access logs retained 2 years running + 5 years archival (para 35A)	Per MoHFW EHR Standards and ECHS Retention Schedule; secure deletion after retention period; audit trail maintained
Restricted (Internal)	Restricted	IT Act 2000; MoD internal security instructions; this SOP	Password-protected storage on authorised systems; email transmission over official channels only	Shredding of physical copies; deletion of digital copies per unit SOP; no special regulatory requirement
Unclassified / Public	Unclassified	General IT Act 2000 obligations; RTI Act 2005 (as applicable)	No special controls; accuracy check before public release	Normal disposal; no special procedure required

80. Handling Procedures

The following handling procedures apply to all information classified RESTRICTED and above:

- **Labelling** — All physical documents and electronic files shall be clearly labelled with their classification marking. Electronic documents shall include the classification in the header or document properties. Reclassification shall be documented and authorised by the originating officer.
- **Storage** — CONFIDENTIAL and above data shall be stored only on authorised, access-controlled systems with encryption enabled (refer Part I, para 12). Physical documents

shall be stored in locked cabinets accessible only to authorised personnel. Portable storage of CONFIDENTIAL or higher data requires explicit authorisation and mandatory encryption.

- **Transmission** — CONFIDENTIAL and above data shall be transmitted only over encrypted channels (TLS 1.2 or above for electronic transmission; sealed physical channels for hard copies). Transmission of CONFIDENTIAL data over personal email, personal messaging applications, or unencrypted channels is strictly prohibited.
- **Access Control** — Access to classified information shall be on a strict need-to-know basis, enforced through RBAC (refer Part I, para 13). Access logs for CONFIDENTIAL and above shall be maintained and reviewed quarterly. Such logs shall be retained as running logs for a minimum of 2 years and archived for a minimum of 5 years in accordance with the ECHS Log Retention Policy (refer Part VI, para 35A). No access shall be granted to third parties without a written data-sharing agreement and, where personal data is involved, the explicit consent of the Data Principal.

81. Disposal and Retention

Information shall be retained only for the period defined in the ECHS Data Retention Schedule (refer Part VII, para 40.8). On expiry of the retention period: physical documents classified CONFIDENTIAL and above shall be destroyed by cross-cut shredding or incineration; digital data shall be securely deleted using approved overwrite tools or degaussing, ensuring it is not recoverable; disposal shall be recorded in the asset/document register. The DPDP Act 2023 requires that personal data be erased as soon as the purpose for which it was collected has been fulfilled and the retention period has expired. No personal data shall be retained indefinitely.

82. Responsibility and Enforcement

Every ECHS officer and employee is individually responsible for correctly classifying information they create and for handling information received from others in accordance with its stated classification. OIC PC is responsible for ensuring compliance with this Policy within their establishment. The DPO shall include information classification audit findings in the quarterly security metrics report to CO ECHS (para 61) and shall maintain the PII Data Classification Register (Annexure D). Any misclassification, unauthorised disclosure, or improper disposal of CONFIDENTIAL or above information shall be treated as a cyber-violation under this SOP and reported per Part X. Violations involving personal data shall additionally be assessed for DPDP Act 2023 breach obligations under para 37.

PART XIV: SECURITY LOGGING AND MONITORING POLICY

Security logs are the primary mechanism for detecting, investigating, and evidencing cyber security incidents and regulatory breaches across ECHS IT infrastructure. This Part establishes mandatory requirements for log generation, collection, protection, retention, real-time monitoring, alerting, roles, and compliance audit. It must be read in conjunction with Part VI para 35A (Log Retention Policy), Part VIII (PII and Health Data Protection), Part X (Cyber Incident Management), and Part XIII (Information Classification Policy).

83. Mandatory Log Sources

Logging shall be enabled and maintained on all ECHS IT assets covering the following mandatory source categories. Disabling logging on any covered system without written authorisation from CO ECHS is a cyber-violation under this SOP. Log data shall flow to centralised or locally managed tamper-evident storage.

- **OS Event Logs** (all workstations and servers) — Login/logout; failed authentication; account create/modify/delete; privilege escalation; service start/stop; system shutdown/restart.
- **Authentication and Identity Logs** — Successful/failed logins; password changes; account lockouts; MFA events; privileged account usage.
- **Network Device Logs** (routers, switches, VPN, VLAN) — Interface state changes; ACL violations; VLAN hop attempts; configuration changes; device restarts.
- **Firewall / IDS / IPS Logs** — Allowed/denied connections; intrusion signatures triggered; traffic anomalies; rule changes.
- **Anti-Malware / EDR Logs** — Malware detections; quarantine actions; scan results; real-time protection status; agent offline events.
- **Health Data Application Logs** (HMIS, claims processing, beneficiary portal, API interfaces) — Record access (read/write/delete); data export; consent management actions; bulk queries; API calls.
- **Email Gateway, Web/Proxy, Backup, and Database Logs** — Phishing detections; URL/category blocks; large data transfers; backup success/failure; schema changes; bulk DB queries on PII/health data.

Any new IT system deployed within ECHS must have logging configured and verified by the Network Administrator before production service. The logging configuration shall be documented in the system's deployment record and reviewed at the next quarterly cyber security audit (para 35).

84. Log Protection and Integrity

All logs shall be stored in tamper-evident storage — acceptable methods include write-once/append-only systems, daily cryptographic hashing, or centralised log aggregation with deletion restricted to the CO ECHS IT Administrator. Read access to logs shall be on a need-to-know basis; deletion requires written authorisation. All ECHS IT systems shall synchronise clocks via a common NTP source; drift exceeding 5 minutes shall be flagged. Each log entry must capture at minimum: timestamp (date, time, timezone), source system/IP, user/process identity, event type, success/failure, and target resource. Logs from health data and PII systems must additionally record the data category accessed. No ECHS personnel shall modify, delete,

suppress, or circumvent log generation on any system; any such tampering shall be reported immediately to the DPO and OIC PC and treated as a HIGH-severity incident under Part X, para 54.

85. Log Retention

All ECHS security logs shall be retained under the two-tier standard established at para 35A of this SOP:

- **Tier 1 — Running Logs**: Minimum 2 years on accessible, queryable online storage from the date of generation. Must be immediately available for monitoring, investigation, and audit without requiring restoration.
- **Tier 2 — Archival Logs**: Minimum 5 years on encrypted offline/cold storage (AES-256 or equivalent). Must be retrievable within 72 hours of an authorised request. A Custody and Integrity Record shall be maintained for each archived log set.
- **Legal Hold**: Logs material to any ongoing incident, inquiry, proceeding, or litigation shall be placed under Legal Hold and shall not be deleted or overwritten regardless of standard retention periods. Legal Hold may be lifted only by written authorisation of the DPO or Legal/Compliance Officer.
- **Disposal**: On expiry of the applicable retention or legal hold period, logs shall be securely deleted (minimum 3-pass DoD wipe for digital media; physical destruction for tape/optical media) and disposal recorded in the Asset and Log Disposal Register. No premature disposal without written authorisation from CO ECHS.

86. Security Monitoring Procedures

Security logs shall be actively monitored to detect events, policy violations, and anomalous behaviour. Systems processing health data, Aadhaar, or PII shall be subject to continuous automated monitoring with alert-based notification to a monitored inbox or dashboard reviewed at least once per duty day. For systems not under continuous monitoring, the Network Administrator shall conduct: daily review of authentication and access logs for health data systems; weekly review of OS event logs, firewall logs, and anti-malware logs for all systems; monthly review of network device configuration change logs. All manual reviews shall be recorded in the Log Review Register. OIC PC shall ensure after-hours coverage arrangements for HIGH/CRITICAL alerts are documented and reviewed quarterly. Where a SIEM or centralised log management platform is deployed, it shall ingest all mandatory log sources within 5 minutes of event generation, maintain correlation rules covering all alerting thresholds at para 87, and restrict admin access to designated CO ECHS IT Administrator and Network Administrators. Where no SIEM exists, CO ECHS shall include centralised log management in its IT roadmap.

87. Alerting Thresholds and Escalation

The following conditions shall trigger an alert requiring immediate action. Alert severity maps to the incident classification at para 54. Any CRITICAL or HIGH alert not resolved within the initial response time shall be escalated as a security incident per Part X.

Trigger / Condition	Severity	Immediate Action	Escalation
5+ failed logins on a single account within 5 minutes	**HIGH**	Auto-lock account; alert Network Admin	OIC PC within 30 min

Trigger / Condition	Severity	Immediate Action	Escalation
Health data system login outside business hours (18:00–08:00)	MEDIUM	Flag for review; log for audit	DPO if access confirmed
Bulk export / query >100 beneficiary records in a session	**HIGH**	Block session; alert DPO immediately	DPO + CO ECHS within 1 hr
Malware detection on any system	**HIGH / CRITICAL**	Isolate system; alert IRT	IRT within 15 min; para 54
Firewall rule change not in change log	**HIGH**	Revert change; investigate	OIC PC + CO ECHS
Anti-malware agent offline >1 hour on any system	MEDIUM	Alert Network Admin to remediate	OIC PC within 2 hrs
Log collection gap >15 min from expected source	MEDIUM	Investigate log agent; check system status	Network Admin within 1 hr
Privileged account used outside approved maintenance window	**HIGH**	Verify with admin; revoke if unconfirmed	OIC PC within 30 min
Data transfer >500 MB to external destination in a session	**HIGH**	Block session; alert DPO	DPO + CO ECHS within 1 hr
Access to minor beneficiary records by non-clinical staff	**HIGH**	Revoke session; alert DPO	DPO within 15 min
Server room physical access after hours (unscheduled)	MEDIUM	Verify with access register; CCTV review	OIC PC within 30 min

88. Linkage to Incident Management

Any log-derived alert not resolved within the initial response time shall be escalated as a security incident per Part X. On incident declaration: (a) the Network Administrator shall immediately apply a Legal Hold on all relevant logs (para 85) and create an integrity-verified snapshot; (b) all relevant logs covering at least 72 hours before the first detected event shall be made available to the Incident Response Team within 2 hours; (c) log evidence, alert details, and monitoring timeline shall be documented in the CIRF (Annexure E), Section B; (d) following resolution, the IRT shall review whether existing log sources, monitoring coverage, or alert thresholds would have enabled earlier detection and shall recommend policy updates if gaps are identified.

89. Roles and Responsibilities

Specific roles and responsibilities for implementation of this Part are as follows:

- **Network Administrator (each PC/RC)** — Configure and maintain log collection; ensure tamper-evident storage; monitor dashboards; respond to alerts; produce log compliance evidence for quarterly audits; manage archival transfers and disposal; maintain Log Review Register.
- **OIC PC** — Overall accountability for logging compliance at their establishment; authorise exceptions; receive HIGH/CRITICAL alerts; ensure after-hours coverage arrangements are documented and reviewed quarterly.
- **Data Protection Officer (DPO)** — Monitor health data and PII-related log alerts; receive escalated data access anomalies; verify log retention compliance at quarterly audit;

maintain Custody and Integrity Register for archived logs; include log compliance metrics in quarterly report to CO ECHS (para 61).

- **All ECHS Personnel** — Never tamper with, delete, or attempt to disable logging on any ECHS system. Report any log manipulation or tampering to the Network Administrator or DPO immediately.

90. Compliance and Audit

Compliance with this Part shall be verified at every quarterly cyber security audit per para 35. The audit shall verify: log sources enabled per para 83; tamper-evident storage in place (para 84); running log retention of 2 years verifiable; archival process operational with Custody and Integrity Records maintained; alert rules configured per para 87; Log Review Register current; no premature log disposal. The DPO shall include log compliance status in the quarterly metrics report to CO ECHS (para 61), covering: log sources active vs. expected; alerts triggered and resolved by severity; legal holds in force; archival transfer status; and identified gaps. This Part shall be reviewed annually or following any significant incident where log coverage or retention was a contributing factor. Failure to implement or maintain requirements under this Part shall be treated as a cyber-violation and may attract disciplinary action; non-compliance involving personal data may additionally attract DPDP Act 2023 penalties.

PART XV: SOFTWARE DEVELOPMENT LIFE CYCLE (SDLC) POLICY

91. Introduction, Scope, and Agency Roles

ECHS does not undertake in-house software development. All IT systems deployed within ECHS infrastructure are procured from external agencies under contract. This Part establishes mandatory security requirements governing the procurement, assessment, deployment, operation, patching, monitoring, and decommissioning of all vendor-supplied software used by ECHS. These requirements apply to every agency supplying or maintaining software on behalf of ECHS, irrespective of contract type or duration.

This Part must be read alongside: Part I (paras 9.2–9.5 — software security), Part VII (para 40.9 — Data Processing Agreements), Part VIII (para 44.1 — third-party data obligations), Part XII (Patch Management Policy), Part XIII (Information Classification Policy), and Part XIV (Security Logging and Monitoring Policy). All security controls applicable to ECHS IT systems under this SOP apply with equal force to software supplied by third-party agencies.

Regulatory basis

DPDP Act 2023 (Sections 8 and 9 — Data Fiduciary security obligations) | IT Act 2000 Section 43A | CERT-In Guidelines on Cybersecurity Incident Reporting | Army Cyber Security Policy 2023 | MoHFW EHR Standards 2023 | ECHS Cyber Security SOP (current version), Parts I, VII, VIII, XII, XIII, XIV

91.1 Defined Agency Roles. For the purposes of this Part, the following role-based designations are used in place of any specific vendor or company name. The agency currently appointed to each role shall be recorded in the ECHS Software Version Register (para 96.4) and updated whenever a new agency is appointed under any role.

Agency Role	Definition
Beneficiary Onboarding and Card Processing Agency	The agency responsible for beneficiary registration, data verification, and ECHS Smart Card printing and issuance.
Bill Processing Agency	The agency responsible for processing cashless claims, medical bills, and reimbursement transactions submitted by empanelled hospitals and beneficiaries.
Primary Healthcare Management Application Agency	The agency developing, hosting, and maintaining the Health Management Information System (HMIS) deployed at ECHS Polyclinics for outpatient management, prescription, and clinical records.
Hospital Empanelment Module Agency	The agency developing and maintaining the module used for hospital empanelment, renewal, and performance monitoring under ECHS.
Beneficiary Portal Agency	The agency responsible for any web or mobile portal through which ECHS beneficiaries access services, view entitlements, or raise grievances.
IT Infrastructure Service Agency	Any agency providing network, server, cloud, or hosting infrastructure services to ECHS, including data centre operators.
Other Empanelled Software Agency	Any other agency contracted to supply, integrate, or maintain software on ECHS IT infrastructure not covered by the roles above.

92. Vendor Software Procurement — Mandatory Security Requirements

All software procured by ECHS for deployment on its IT infrastructure — regardless of which agency role supplies it — shall satisfy the following security requirements before procurement approval is granted. These requirements shall be incorporated into the Request for Proposal (RFP) or tender documents and evaluated as scored technical criteria. Failure to meet a Mandatory requirement shall disqualify the agency from selection unless a formal waiver is approved in writing by the Dir (Stats and Automation), CO ECHS prior to evaluation.

Requirement	Standard / Expectation	Status
Authentication and access control	Role-based access control (RBAC); passwords compliant with Part XI para 63; MFA mandatory for administrative accounts and all accounts accessing health data or PII.	**Mandatory**
Data encryption	PII and health data encrypted at rest (AES-256 or equivalent) and in transit (TLS 1.2+); Aadhaar numbers stored in masked or tokenised form only (Part XIII para 78).	**Mandatory**
Audit logging	Generates tamper-evident logs covering all event categories in Part XIV para 83; logs exportable for ECHS log management integration; retention configurable to 2-year running / 5-year archival (para 35A).	**Mandatory**
Session management	Auto-timeout after 5 minutes of inactivity (para 46.8); session tokens invalidated on logout; no persistent session tokens.	**Mandatory**
Input validation and application security	Protection against OWASP Top-10 vulnerabilities; validated inputs on all user-facing fields; no SQL injection, XSS, or CSRF vulnerabilities in production.	**Mandatory**
Security patch support	Agency commits to patch delivery per Part XII para 69 timelines: Critical within 72 hrs; High within 7 days; Medium/Low within 30 days. Minimum software support lifecycle of 3 years from deployment.	**Mandatory**
DPDP Act 2023 compliance	Software supports lawful purpose collection, consent capture, data minimisation, purpose limitation, and erasure/return on request under the DPDP Act 2023.	**Mandatory**
Vulnerability disclosure	Agency has a documented CVE response process; commits to notifying CO ECHS within 24 hours of discovery of any Critical vulnerability affecting deployed software or ECHS data.	**Mandatory**
Data residency	All ECHS beneficiary data processed and stored within Indian jurisdiction; no cross-border transfer without explicit CO ECHS authorisation and DPDP Act compliance.	**Mandatory**
Independent VAPT	Software subjected to independent VAPT within the preceding 12 months; report available to ECHS on request; all Critical and High findings remediated before deployment.	**Recommended**
Source code escrow	For the Primary Healthcare Management Application Agency and the Beneficiary Onboarding and Card Processing Agency, a source code escrow arrangement	**Recommended**

Requirement	Standard / Expectation	Status
	shall be included in the contract.	

93. Pre-Procurement Security Assessment (PPSA)

Before any software is approved for deployment on ECHS infrastructure, a Pre-Procurement Security Assessment (PPSA) shall be conducted by the Network Administrator at CO ECHS in co-ordination with the DPO. The PPSA is mandatory for every agency role listed at para 91.1 and shall cover the following:

- **Data flow mapping.** Identify all categories of ECHS data the software will access, process, store, or transmit. Classify data per Part XIII (para 78) — Aadhaar, PII, health records, or CONFIDENTIAL — and document all data flows into and out of the software.
- **Agency security questionnaire.** The agency shall complete a standardised security questionnaire covering authentication, encryption, logging, incident response, patch management, DPDP compliance, and data residency. Unsatisfactory responses or non-response are grounds for disqualification.
- **VAPT evidence review.** Review any VAPT report provided by the agency. For the Primary Healthcare Management Application Agency and the Bill Processing Agency, where no current VAPT report exists, ECHS shall commission an independent VAPT by a CERT-In empanelled organisation before final approval.
- **DPDP Act 2023 compliance check.** Assess whether the software supports consent capture, data minimisation, erasure on request, and breach notification capability as required under the DPDP Act 2023 (Part VII).
- **Compatibility and integration check.** Verify compatibility with ECHS IT infrastructure, operating system versions, network architecture, and existing security tools. Confirm the software's log output can be integrated with ECHS log management from day one of deployment.
- **Risk assessment and sign-off.** Document residual risks identified during the PPSA and proposed mitigating controls. The PPSA report shall be signed by the Dir (Stats and Automation), CO ECHS before deployment approval is granted. The signed PPSA shall be filed and produced at every quarterly cyber security audit (para 35).

94. Contractual and Legal Obligations

All contracts with agencies supplying software to ECHS shall include the following mandatory clauses, in addition to the Data Processing Agreement (DPA) required under para 40.9:

- **Security standards compliance.** The agency warrants that the software meets all requirements in para 92 at the time of deployment and shall maintain compliance throughout the contract term. Any lapse in compliance shall be notified to CO ECHS within 48 hours of discovery.
- **Security incident notification.** The agency shall notify CO ECHS within 24 hours of discovering any security incident, data breach, or Critical or High vulnerability (CVSS score ≥ 7.0) affecting the deployed software or any ECHS data processed under the contract.

- **Patch delivery obligation.** The agency commits to delivering security patches within the timelines in Part XII para 69 throughout the support lifecycle. Failure to deliver a Critical patch within 72 hours without a documented and accepted reason shall constitute a material breach of contract.
- **Audit rights.** CO ECHS reserves the right to conduct or commission an independent security audit of the agency's software and data handling practices at any time during the contract term with reasonable notice. The agency shall provide full co-operation and access to relevant systems, personnel, and documentation.
- **Data return and deletion.** On contract termination or expiry, the agency shall return all ECHS data in a machine-readable format within 15 days and securely delete all copies from agency systems within 30 days, providing CO ECHS with a written certificate of deletion.
- **Sub-processor controls.** The agency shall not transfer or sub-process ECHS data to any third party without prior written approval from CO ECHS. Approved sub-processors are bound by the same data protection obligations as the contracting agency.
- **Governing law and jurisdiction.** The contract shall be governed by Indian law. All disputes shall be subject to the jurisdiction of competent Indian courts.

95. Secure Deployment and Configuration

Deployment of any new or updated software on ECHS infrastructure shall follow the controlled change management process at para 29 and satisfy all of the following requirements before go-live:

- **Default credential change.** All agency-supplied default usernames, passwords, and API keys shall be changed before go-live in compliance with Part XI (Password Management Policy, paras 62–68).
- **Least-privilege configuration.** Application service accounts shall be granted only the permissions required for their defined function. Administrative accounts shall be separate from end-user accounts. No shared privileged credentials are permitted.
- **Unnecessary features and services disabled.** All software features, ports, protocols, and services not required for ECHS operations shall be disabled before deployment. Demo modes, test accounts, and trial features shall be removed from production environments.
- **Network segmentation.** Software accessing health data or PII shall be deployed on an isolated VLAN per para 17. External-facing APIs shall be placed behind the ECHS firewall with documented access control rules reviewed and approved by the Network Administrator.
- **Logging integration verified.** The software's audit log output shall be verified as flowing into ECHS log management before go-live. Log format, tamper-evident storage, and export mechanism shall be confirmed and documented.
- **User Acceptance Testing (UAT) security validation.** UAT shall include explicit verification of: RBAC and authentication controls; data encryption in transit and at rest; session timeout behaviour; and correct functioning of all security features required under para 92. UAT sign-off shall be documented.

- **Go-live approval.** Written go-live approval from the OIC PC (or Dir Stats and Automation for CO ECHS-level deployments) is required before any software is placed into production. The approval record shall be filed and produced at the next quarterly cyber security audit (para 35).

96. Vulnerability and Patch Management for Agency-Supplied Software

All agency-supplied software is subject to the patch management requirements in Part XII (paras 69–75). The following additional controls apply specifically to third-party software:

- **Advisory monitoring.** The Network Administrator shall subscribe to vendor security advisories, CVE bulletins, and CERT-In alerts for every deployed agency software product. Critical and High vulnerabilities shall be risk-assessed within 24 hours of discovery.
- **Agency patch co-ordination.** For Critical vulnerabilities, ECHS shall contact the responsible agency immediately to confirm patch availability and delivery timeline. Where a patch is not available within the 72-hour window, compensating controls (such as network isolation or access restriction) shall be applied and the exception documented per Part XII para 74.
- **Pre-deployment testing.** Patches to the Primary Healthcare Management Application and the Bill Processing system shall be tested in a staging or UAT environment before production deployment, unless the severity of the vulnerability warrants direct production deployment (the decision to bypass testing must be documented and approved by the Network Administrator).
- **Software Version Register.** The Network Administrator shall maintain a Software Version Register recording for each deployed application: product name, agency role, current version in production, date of last patch applied, next scheduled review date, and end-of-support date. The Register shall be produced at every quarterly cyber security audit (para 35).
- **End-of-support tracking.** Software approaching end-of-support (within 6 months) shall be flagged to the Dir (Stats and Automation), CO ECHS for procurement or upgrade planning. Continued use of out-of-support software on systems processing PII or health data is not permitted without a risk-acceptance waiver approved in writing by CO ECHS.

97. Third-Party Software Security Monitoring

Agency-supplied software shall be subject to all monitoring requirements in Part XIV (Security Logging and Monitoring Policy) and additionally:

- **Periodic VAPT.** The Primary Healthcare Management Application, the Bill Processing system, and the Beneficiary Onboarding and Card Processing system shall each be subjected to an independent VAPT at least once every two years, or following any significant security incident involving that software. VAPT shall be conducted by a CERT-In empanelled security testing organisation. All Critical and High findings shall be remediated within the timelines in Part XII para 69. A VAPT closure report shall be filed with CO ECHS.
- **Application behaviour monitoring.** Anomalous application behaviour — including unexpected external network connections, unusual data access volumes, bulk exports,

or API calls outside normal operational parameters — shall be flagged per the alerting thresholds at Part XIV para 87.

- **Agency remote access controls.** Any remote access granted to an agency for support or maintenance shall be: time-limited and approved in advance by the OIC PC or Network Administrator; conducted over an approved, monitored channel; logged in full per Part XIV para 83; and revoked immediately upon completion of the support activity. No agency remote access session shall be left open or unattended. A record of every remote access session shall be maintained.
- **Supply chain review.** Where a software update from an agency introduces new third-party components or dependencies, the Network Administrator shall review the release notes. For the Primary Healthcare Management Application, Bill Processing system, and Beneficiary Onboarding and Card Processing system, a lightweight security review shall be performed before the update is deployed in production.

98. Software Decommissioning and End-of-Life

When any agency-supplied software reaches end-of-life or is being replaced, the following decommissioning controls shall apply before the software is shut down:

- **Data export and retention check.** All ECHS data held within the software shall be exported, classified per Part XIII, and retained or disposed of in accordance with the Data Retention Schedule (para 40.8) and DPDP Act 2023 erasure obligations (para 43) before decommissioning proceeds.
- **Agency data deletion verification.** Written confirmation from the agency that all copies of ECHS data on agency systems have been securely deleted shall be obtained within 30 days of contract termination, per the obligation at para 94.
- **Credential and access revocation.** All service accounts, API credentials, integration tokens, and user accounts associated with the decommissioned software shall be revoked on the day of decommissioning. The Network Administrator shall verify and log each revocation.
- **Log archival before shutdown.** All logs generated by the decommissioned software shall be transferred to archival storage per para 35A before the software is shut down. The 5-year archival retention obligation continues after decommissioning.
- **Registers updated.** The decommissioned software shall be removed from the Software Version Register and the ECHS Asset Register (para 22) within 5 working days of decommissioning. A decommissioning completion record shall be filed and produced at the next quarterly audit.
- **Network and firewall cleanup.** All firewall rules, VLAN configurations, API gateway entries, and network exceptions created for the decommissioned software shall be removed within 5 working days. The Network Administrator shall confirm and document completion of cleanup.

99. Roles, Responsibilities, and Compliance Audit

The following roles and responsibilities apply to the implementation of this Part across all ECHS establishments:

Role	Responsibilities under this Part
Dir (Stats and Automation), CO ECHS	Policy owner. Sign off all Pre-Procurement Security Assessments (para 93). Approve exceptions and risk-acceptance waivers. Authorise continued use of out-of-support software. Review quarterly SDLC compliance metrics.
Network Administrator, CO ECHS	Conduct PPSA (para 93). Maintain Software Version Register (para 96.4). Monitor advisories and apply patches per Part XII. Manage and log agency remote access. Co-ordinate VAPT. Execute decommissioning checklist. Verify log integration at every deployment.
Data Protection Officer (DPO)	Review DPDP compliance aspects of all procured software. Ensure Data Processing Agreements are in place (para 40.9). Monitor data access logs for agency software. Verify data deletion certificates on contract termination. Include SDLC metrics in quarterly report to CO ECHS (para 61).
OIC PC	Authorise go-live of agency software at PC level. Report any suspected security issue with agency software to CO ECHS Network Administrator immediately. Verify logging is operational before authorising go-live.
Procurement / Contracting Authority	Incorporate security requirements (para 92) into all RFPs and tender documents. Ensure mandatory contractual clauses (para 94) and Data Processing Agreement (para 40.9) are included before contract execution. Co-ordinate with DPO and Network Administrator during procurement evaluation.
All Contracted Agencies	Meet all requirements in para 92 as a condition of contract. Deliver patches within prescribed timelines. Notify CO ECHS of security incidents within 24 hours. Co-operate fully with ECHS security audits and VAPT. Comply with data return and deletion obligations on contract termination.

Compliance with this Part shall be verified at every quarterly cyber security audit (para 35). The DPO shall include SDLC compliance metrics in the quarterly report to CO ECHS (para 61), covering: PPSAs completed and signed off; outstanding security requirement gaps for any deployed agency application; patch compliance status per agency; VAPT status and outstanding findings; end-of-support flags; and decommissioning actions completed or pending. Non-compliance with this Part by ECHS personnel shall be treated as a cyber-violation under this SOP and may attract disciplinary action. Non-compliance by a contracted agency shall constitute a material breach of contract and may result in contract termination and reporting to the appropriate regulatory authority.

PART XVI: RISK ASSESSMENT AND MANAGEMENT POLICY

100. Introduction

Cyber risk is inherent in all IT operations of ECHS. As a Data Fiduciary under the DPDP Act 2023 processing health records, Aadhaar-linked data, and financial transactions of retired defence personnel, ECHS must systematically identify, assess, treat, and monitor cyber risks to its IT assets and the personal data entrusted to it. This Annexure establishes the mandatory Risk Assessment and Management Policy (RAMP) for ECHS, aligned with the ISO/IEC 27005 risk management framework and the obligations of the DPDP Act 2023, IT Act 2000 Section 43A, and the Army Cyber Security Policy 2023.

101. Scope

This Policy applies to all ECHS IT assets, information systems, agency-supplied software, and data processing activities across CO ECHS, all Regional Centres (RCs), and all Polyclinics (PCs). It covers risks to the Confidentiality, Integrity, and Availability (CIA) of ECHS information assets, including PII, health records, Aadhaar data, financial claims data, and IT infrastructure.

102. Risk Assessment Process

Risk assessments shall be conducted using the following five-step process:

- **Step 1 — Asset Identification.** Identify all ECHS IT assets, information assets, and data categories in scope, using the Asset Register (para 22 of the SOP) as the baseline.
- **Step 2 — Threat and Vulnerability Identification.** Identify threats (internal, external, technical, human) and vulnerabilities applicable to each asset. Sources include: CERT-In advisories, VAPT findings (Part XV para 97), incident history (Part X), and vendor security bulletins (Part XV para 96).
- **Step 3 — Risk Scoring.** Score each identified risk using the Risk Matrix at para 4 below. Risk Score = Likelihood (L) x Impact (I), each rated 1–5.
- **Step 4 — Risk Treatment.** Select and implement treatment per the Response and Escalation Table at para 5 below. Treatment options: Mitigate (apply controls); Transfer (insure / contract); Accept (with documented justification); Avoid (discontinue activity).
- **Step 5 — Monitoring and Review.** Record all risks, treatment actions, and residual scores in the ECHS Risk Register (para 6). Review the Risk Register at every quarterly cyber security audit (para 35) and update following any significant incident.

103. Risk Scoring Matrix

Risk Score = Likelihood (1–5) x Impact (1–5). Likelihood and Impact definitions are given below the matrix.

Likelihood \ Impact	Negligible (1)	Minor (2)	Moderate (3)	Major (4)	Critical (5)
Almost Certain (5)	5	10	15	20	25
Likely (4)	4	8	12	16	20
Possible (3)	3	6	9	12	15
Unlikely (2)	2	4	6	8	10
Rare (1)	1	2	3	4	5

Likelihood Score	Level	Definition
5	**Almost Certain**	Expected to occur in most circumstances — once or more per year within ECHS.
4	**Likely**	Will probably occur — once every 1–2 years.
3	**Possible**	Could occur at some time — once every 2–5 years.
2	**Unlikely**	Not expected but conceivable — once every 5–10 years.
1	**Rare**	May occur only in exceptional circumstances — less than once in 10 years.

Impact Score	Level	Definition
5	**Critical**	Catastrophic — mass PII/health data breach; severe regulatory penalty; prolonged service outage; irreversible reputational damage.
4	**Major**	Significant — large-scale data breach affecting many beneficiaries; substantial financial loss; major service disruption.
3	**Moderate**	Moderate — limited data breach; financial loss; temporary service disruption; regulatory notice issued.
2	**Minor**	Minor — small-scale incident; minimal data exposure; short service disruption; manageable financial impact.
1	**Negligible**	Negligible — near-miss or contained incident; no data loss; no service impact; no regulatory consequence.

Score Range	Rating	Colour Code	Required Action
17 – 25	**CRITICAL**	Red	Immediate escalation; emergency treatment; halt operations if necessary.
10 – 16	**HIGH**	Orange	Priority treatment; escalate to Dir Stats & Automation within 24 hours.
5 – 9	**MEDIUM**	Yellow	Treatment plan within 30 days; quarterly review.
1 – 4	**LOW**	Green	Accept or monitor; annual review.

104. Risk Response and Escalation Requirements

Risk Score / Rating	Response and Escalation Requirements
CRITICAL (17–25)	Immediate escalation to CO ECHS MD. Emergency response within 2 hours. Risk must be reduced before operations continue. Treat as P1 incident (SOP para 54).
HIGH (10–16)	Escalate to Dir (Stats & Automation) within 24 hours. Mandatory treatment plan within 5 working days. Monthly progress review.
MEDIUM (5–9)	Assign owner. Treatment plan within 30 days. Quarterly progress review at cyber security audit (para 35).

Risk Score / Rating	Response and Escalation Requirements
LOW (1–4)	Accept or monitor. Document acceptance in Risk Register. Annual review.

105. ECHS IT Cyber Risk Register

The following Risk Register records the identified cyber risks to ECHS IT operations, their inherent risk scores, applied controls, and residual risk ratings. The Risk Register shall be reviewed and updated at every quarterly cyber security audit (para 35). New risks identified through incidents, VAPT, or threat intelligence shall be added immediately. The DPO shall include risk register status in the quarterly metrics report to CO ECHS (para 61).

Risk ID	Risk Description	Cause / Threat Source	Inherent Risk Rating	Likeli-hood (L)	Impact (I)	Risk Score (LxI)	Controls / Mitigating Measures	Residual Risk Rating	Resi-dual L	Resi-dual I	Resi-dual Score
ECHS-R-001	Unauthorised access to beneficiary health records	Weak authentication; shared credentials	HIGH	4	4	16	MFA; RBAC; access logging (Part XIV); password policy (Part XI)	**HIGH**	2	4	8
ECHS-R-002	Aadhaar data breach during eSatyapan authentication	API vulnerabilities; insecure transmission	HIGH	3	5	15	TLS 1.2+; tokenisation; UIDAI API audit; Annexure H reporting	**MEDIUM**	2	4	8
ECHS-R-003	Ransomware / malware infection on ECHS workstations	Phishing; unpatched systems; USB media	HIGH	4	4	16	Anti-malware; patch management (Part XII); USB restriction; staff training	**MEDIUM**	2	3	6
ECHS-R-004	Fraudulent cashless claims submitted via Bill Processing Agency interface	Weak input validation; collusion	HIGH	3	4	12	AI-based fraud analytics; anomaly alerting (Part XIV para 87); VAPT (Part XV)	**LOW**	2	3	6
ECHS-R-005	Insider threat — misuse of privileged access by IT Administrator	Unchecked admin rights; no monitoring	MEDIUM	2	5	10	UPM Proforma; PAM controls; quarterly access review; audit logging	**LOW**	1	4	4
ECHS-R-006	Data loss due to inadequate backup or failed	No tested backup; single point of failure	MEDIUM	3	4	12	Backup logs (Part XIV para 83); quarterly	**LOW**	2	3	6

Risk ID	Risk Description	Cause / Threat Source	Inherent Risk Rating	Likeli-hood (L)	Impact (I)	Risk Score (LxI)	Controls / Mitigating Measures	Residual Risk Rating	Resi-dual L	Resi-dual I	Resi-dual Score
	recovery						recovery drills; para 35A retention				
ECHS-R-007	Non-compliance with DPDP Act 2023 — inadequate consent or data retention	Gaps in consent management; over-retention	HIGH	3	4	12	Consent Forms (Annexures A/B); Retention Schedule (para 40.8); DPO oversight	**LOW**	1	4	4
ECHS-R-008	Vendor / agency software vulnerability — Primary Healthcare Management Application	Unpatched third-party software	HIGH	3	4	12	Biennial VAPT (Part XV para 97); patch SLAs in contract (Part XV para 94)	**MEDIUM**	2	3	6
ECHS-R-009	Physical unauthorised access to server room / data centre	Weak physical access control; tailgating	MEDIUM	2	4	8	Access logs; CCTV monitoring (Part XIV para 83); after-hours alerts (para 87)	**LOW**	1	4	4
ECHS-R-010	Log tampering or deletion — loss of audit trail	Insider threat; malware; misconfiguration	MEDIUM	2	5	10	Tamper-evident storage (Part XIV para 84); immutable log management; Legal Hold	**LOW**	1	4	4

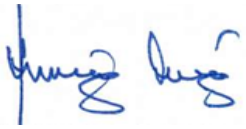
106. Roles and Responsibilities

Role	Responsibilities under this Policy
Dir (Stats & Automation), CO ECHS	Policy owner. Review and approve Risk Register updates. Receive HIGH and CRITICAL risk escalations. Authorise risk acceptance for residual HIGH risks. Include risk summary in quarterly CO ECHS briefings.
Data Protection Officer (DPO)	Ensure risks to PII, Aadhaar, and health data are assessed and treated. Monitor DPDP Act 2023 compliance risks. Report risk register status in quarterly metrics report to CO ECHS (para 61).
Network Administrator (CO	Identify and log new risks arising from IT operations. Implement assigned

Role	Responsibilities under this Policy
ECHS / RC)	treatment controls. Maintain evidence of control effectiveness for quarterly audit. Report new threats from vendor advisories and CERT-In.
OIC PC	Identify and report local risks to Network Administrator. Ensure IT controls at PC level address assigned risks. Report any risk materialising as an incident per Part X.
All ECHS Personnel	Report any observed threat, vulnerability, or near-miss to the Network Administrator or DPO. Co-operate with risk assessment exercises and annual reviews.

107. Review and Maintenance

The Risk Register and this Policy shall be reviewed: (a) at every quarterly cyber security audit (para 35); (b) following any P1 or P2 security incident (para 54); (c) following any VAPT (Part XV para 97); (d) whenever a significant change is made to ECHS IT infrastructure or agency software deployments; and (e) at minimum annually. Updates to the Risk Register require approval of the Dir (Stats & Automation), CO ECHS. Major revisions to this Policy require Dy MD approval via a noting sheet.



(Anurag Bhardwaj)
Col
Dir (Stats & Automation)
20 Jul 2026

Distr:
All Br/Sec, CO ECHS
All RCs/PC
Data Protection Officer, CO ECHS

ANNEXURE A

DPDP CONSENT FORM TEMPLATE — ADULT BENEFICIARY

(To be obtained in duplicate at time of enrolment and upon any change in data processing purpose)

ECHS — PERSONAL DATA CONSENT FORM (ADULT BENEFICIARY)

File No: B/49722-IT/CONSENT/AG/ECHS

NOTICE TO DATA PRINCIPAL

Ex-Servicemen Contributory Health Scheme (ECHS), as a Data Fiduciary under the Digital Personal Data Protection Act 2023, is collecting your personal data (including health/medical data) for the purpose of providing healthcare services to you and your enrolled dependents. Your data will be processed for: registration and authentication; medical record maintenance; referral to empaneled hospitals; administrative correspondence; and compliance with statutory obligations.

Your data will not be shared with any third party except empaneled hospitals/labs (for treatment), government agencies (as required by law), or as directed by a competent court. You have the right to access, correct, and erase your data, and to withdraw consent at any time by contacting the DPO at CO ECHS, Delhi Cantt-10.

CONSENT DECLARATION

I, _____ (Name), Service No/ECHS Card No _____, having been informed of my rights and the purpose of data collection, hereby freely give my consent to ECHS to collect, store, process, and share (as stated above) my personal data including health/medical data for the purposes of availing ECHS healthcare services.

I understand I may withdraw this consent at any time by writing to the Data Protection Officer, ECHS.

Signature / Thumb Impression: _____ Date: _____

Witness (ECHS Staff): _____ Designation: _____

ANNEXURE B

DPDP CONSENT FORM TEMPLATE — MINOR BENEFICIARY / GUARDIAN

(Same is to be implemented by all software/ applications)

(To be obtained from the Parent/Lawful Guardian of every minor beneficiary below 18 years of age)

ECHS — PARENTAL / GUARDIAN CONSENT FOR MINOR BENEFICIARY

File No: B/49722-IT/CONSENT-MINOR/AG/ECHS

NOTICE TO PARENT/GUARDIAN

ECHS is collecting personal data (including health/medical data) of the above-named minor beneficiary under your guardianship for the purpose of providing healthcare services. Under Section 9 of the Digital Personal Data Protection Act 2023, your verifiable consent as parent/lawful guardian is required before any personal data of a child (below 18 years) is processed.

Minor Beneficiary Name: _____ Date of Birth: _____

ECHS Card No: _____ Relationship to Minor: _____

Age Verification Document: Aadhaar / Birth Certificate / School Certificate (circle one)

PARENTAL/GUARDIAN CONSENT DECLARATION

I, _____ (Parent/Guardian Name), being the lawful guardian of the above-named minor, hereby freely give my verifiable consent to ECHS to collect, store, process and share the personal data including health/medical data of the minor named above, for the purpose of availing ECHS healthcare services.

I acknowledge that upon the minor attaining 18 years of age, this consent shall cease to be valid and fresh consent shall be sought from the beneficiary in their own right.

Signature / Thumb Impression of Parent/Guardian: _____ Date: _____

Identity Proof (Type & No.): _____

Witness (ECHS Staff): _____ Designation: _____

ANNEXURE C

DATA BREACH RESPONSE PROTOCOL

In the event of a personal data breach involving PII or health data of ECHS beneficiaries, the following seven-step protocol must be activated immediately:

Step	Timeline	Action	Responsible Party
1	Immediate (0–1 hr)	Contain the breach: isolate affected systems, disable compromised accounts, preserve forensic evidence. Do NOT delete data.	OIC PC / Network Admin
2	Within 6 hours	Report to DPO at CO ECHS with: nature of breach, data affected, estimated number of Data Principals affected, whether minor data is involved.	OIC PC / Dir RC
3	Within 24 hours	Report to CERT-Army per existing incident reporting protocol. If minor beneficiary data is involved, notify parent/guardian immediately.	DPO / CO ECHS
4	Within 72 hours	File report with Data Protection Board of India (DPBI) if breach is likely to result in harm to Data Principals. Use DPBI prescribed format.	DPO / CO ECHS
5	Within 7 days	Notify all affected Data Principals individually: nature of breach, data affected, ECHS steps taken, self-protection guidance, DPO contact.	DPO
6	Within 30 days	Complete root cause analysis. Implement remediation measures. Submit lessons-learned report to CO ECHS.	DPO / IT Team
7	Ongoing	Maintain breach register. Cooperate with any DPBI/CERT-In investigation. Update controls to prevent recurrence.	DPO

ANNEXURE D

PII DATA CLASSIFICATION REGISTER (TEMPLATE)

(To be maintained by the Data Protection Officer; reviewed and updated quarterly)

S. No	System / Database Name	PII Category Held	Includes Minor Data?	Classification Level	Encryption Status	Data Owner / Custodian
1						
2						
3						
4						
5						

ANNEXURE E

CYBER INCIDENT REPORT FORMAT (CIRF) — INTERNAL

(For all P1, P2 and P3 incidents. P4 incidents may be reported via monthly Incident Register summary)

CYBER INCIDENT REPORT FORMAT (CIRF) — INTERNAL

CO ECHS | File No: B/49722-IT/CIRF/AG/ECHS

SECTION A — INCIDENT IDENTIFICATION

IRN: ECHS / _____ / _____ / _____ Date of Report: _____

Date & Time of Detection: _____ Date & Time of Occurrence (if known): _____ Reporting Unit / PC / RC: _____ Location: _____
Reported by (Name, Rank, Appointment): _____

Severity Level (circle): CRITICAL (P1) / HIGH (P2) / MEDIUM (P3)

SECTION B — INCIDENT DESCRIPTION

Type of Incident (tick all that apply):

[ ] Malware/Ransomware [ ] Unauthorised Access [ ] Phishing [ ] Data Breach/Exfiltration

[ ] USB/Air-Gap Violation [ ] Insider Threat [ ] Physical Theft [ ] DoS/DDoS [ ] Other: ___

Systems / Assets Affected:
_____

How was the incident detected:
_____?

Brief Description
_____
_____

SECTION C — PII / PERSONAL DATA BREACH ASSESSMENT

Personal data of beneficiaries involved? YES /NO/UNDER INVESTIGATION (circle)
Data categories (tick all that apply):

[ ] Health/Medical Records [ ] Aadhaar/Identity [ ] Financial Data [ ] Contact Details

[ ] Biometric Data [ ] Minor Beneficiary Data [ ] Service Records [ ] Other: _____

Estimated no. of beneficiaries affected: _____ Minors among them: _____

DPO notified? YES / NO Time of notification: _____ DPO Name: _____

Nature of potential harm to Data Principals: _____

SECTION D — CONTAINMENT AND ACTIONS TAKEN

Containment Status: CONTAINED / PARTIALLY CONTAINED / NOT YET CONTAINED (circle)

Actions taken (with timestamps):

1. _____

2. _____

3. _____

SECTION E — REGULATORY NOTIFICATIONS

CERT-Army notified? YES/NO Date/Time: _____ Ack Ref No: _____

CERT-In notified (if applicable)? YES/NO Date/Time: _____ Filing Ref No: _____

DPBI notified? YES/NO Date/Time: _____ Filing Reference No: _____

Affected beneficiaries notified? YES / NO / PENDING Method: _____

SECTION F — SIGNATURES

Reported by: _____ Signature: _____ Date: _____

IT / Network Lead: _____ Signature: _____ Date: _____
DPO (if PII breach): _____ Signature: _____ Date: _____
Incident Commander: _____ Signature: _____ Date: _____

ANNEXURE F

CERT-In CYBER SECURITY INCIDENT REPORT FORMAT

(As per CERT-In Directions under Section 70B of the Information Technology Act 2000 | Report to: incident@cert-in.org.in)

CERT-In Mandatory Reporting Obligation
Under the CERT-In Directions dated 28 April 2022 (as amended), all government entities including defence establishments must mandatorily report cyber security incidents to CERT-In within 6 hours of noticing such incidents or being brought to notice about such incidents. Failure to report is a violation of the IT Act 2000. ECHS officers must use this format for all mandatory CERT-In notifications.

CERT-In CYBER SECURITY INCIDENT REPORT

Submit to: incident@cert-in.org.in | Helpdesk: 1800-11-4949 | Fax: 1800-11-6969

PART I — REPORTING ORGANISATION DETAILS

Organisation Name: Ex-Servicemen Contributory Health Scheme (CO ECHS)
Organisation Type: Government — Ministry of Defence, Government of India
Address: CO ECHS, ECHS Bhawan, Delhi Cantt-10, New Delhi — 110010

Contact Person (Nodal Officer / DPO):
_____

Designation: _____ Phone: _____ Email: _____ Reporting Unit (RC / PC / CO ECHS):
_____

Date and Time of This Report: _____

PART II — INCIDENT DETAILS

Date and Time of Incident (when noticed): _____

Date and Time of Incident (when occurred, if known): _____

Type of Incident (as per CERT-In categories — tick applicable):

[ ] Malicious Code (Virus / Worm / Trojan / Ransomware / Spyware / Adware / Rootkit)
[ ] Denial of Service (DoS) / Distributed Denial of Service (DDoS)
[ ] Intrusion / Hacking / Unauthorised Access (System or Network)
[ ] Data Breach / Data Leak / Unauthorised Data Exfiltration
[ ] Phishing / Spear Phishing / Social Engineering Attack

[ ] Website Defacement / Compromise of Government Website
[ ] Targeted Scanning / Probing of Critical Networks / IT Infrastructure
[ ] Identity Theft / Credential Compromise
[ ] Counterfeit Mobile Apps / Fake Websites Impersonating ECHS
[ ] Attacks on Internet of Things (IoT) Devices / Medical Devices / Healthcare Systems
[ ] Compromise of Critical Information Infrastructure [ ] Other (Specify): _____

Brief Description of the Incident (what happened, systems affected, impact observed):
_____
_____
_____

PART III — AFFECTED SYSTEMS / INFRASTRUCTURE

I
P Addresses of Affected Systems (if known):
_____

Hostnames / System Names:
_____

Operating Systems and Versions:
_____

Applications / Software Affected:
_____

Network Segment Affected:
_____

Is this system connected to the internet? YES / NO / PARTIALLY (circle)

PART IV — ATTACKER / THREAT ACTOR INFORMATION (if known)

Source IP Address(es):
_____

Attacker Domain / URL (if known):
_____

Malware Hashes / Indicators of Compromise (IOCs):
_____
Country of Origin (if determinable):
_____

PART V — PERSONAL DATA / HEALTH DATA IMPACT (DPDP Consideration)

Personal data of beneficiaries compromised? YES / NO / UNDER INVESTIGATION (circle)

If YES, categories of data (tick all that apply):

[ ] Health / Medical Records [ ] Aadhaar / Identity [ ] Financial Data [ ] Biometric Data
[ ] Minor Beneficiary Data [ ] Contact / Demographic Data [ ] Other: _____

Approximate no. of individuals whose data is affected: _____

Has the Data Protection Board of India (DPBI) been notified? YES / NO (circle)

PART VI — RESPONSE ACTIONS TAKEN

Immediate actions taken to contain the incident: _____
_____
_____
_____

Current status of incident: CONTAINED / ONGOING / RESOLVED (circle)

Assistance / technical support required from CERT-In: YES / NO (if YES, describe below): _____
_____

PART VII — LOG / EVIDENCE INFORMATION

Are system / network logs available? YES / NO / PARTIALLY (circle)

Log time period available: From _____ To _____

Are logs / evidence preserved for forensic analysis? YES / NO (circle)

PART VIII — DECLARATION

I hereby declare that the information furnished above is true and correct to the best of my knowledge. I understand that any false reporting may attract action under the Information Technology Act 2000 and applicable regulations.

Name: _____ Designation:

_____

Signature: _____ Date: _____ Time: _____

Authorised by (Incident Commander): _____

FOR CERT-In USE ONLY

Acknowledgement No: _____ Date Received: _____

Assigned

Analyst: _____