CHAPTER [8]: NETWORK TECHNOLOGY GOVERNANCE, CERTIFICATION AND AUDIT

8. Network Technology Governance, Certification and Audit

All Network Participants and Ecosystem Participants[1] must ensure the security of End User data that is processed or transmitted through the ONDC Network in compliance with the Applicable Laws and the ONDC Network Policy.

8.1. Implementing Reasonable Security Practices and Procedures

8.1.1. Network Participants will be responsible for the implementation of reasonable security practices and standards as provided in Clause 8.1.2 and have a comprehensive, documented information security programme (including, but not limited to, standard operating procedures, security principles and clearly defined chain of command) and policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business.

8.1.2. For the security practices and standards, Network Participants must implement the safeguards that are no less rigorous than the accepted industry practices, including the international standards IS/ISO/IEC 27001 and COBIT, or any other equivalent or higher standard or any other standard as prescribed under Applicable Law.

8.1.3. If a Network Participant engages any Ecosystem Participant, such as a Technology Service Provider, for offering its services or products on the ONDC Network, it shall ensure that such Ecosystem Participant also complies with the clauses of this Chapter.

8.2. Security Breach Procedure

8.2.1. If a Network Participant becomes aware of a cyber security incident originating in/from their system, it must report the incident to the Competent Authorities within the prescribed time period as may be required under Applicable Laws.

8.2.2. If Confidential Information or End User data may have been accessed, disclosed, or acquired without proper authorization and contrary to the terms of the Applicable Law, Network Participant Agreement or the Network Policy ("Data Breach"), such Network Participant must alert ONDC of such Data Breach or cyber security incident within 6 hours of being aware of such Data Breach.

8.2.3. Network Participant must provide ONDC with all information reasonably necessary to fully understand the nature and scope of the Data Breach. ONDC shall prescribe the format and procedure for such reporting through a circular published on the ONDC website.

8.2.4. Network Participant should on a best effort basis attempt to immediately prevent any attempt of unauthorised access or disclosure of the Confidential Information or End User data and take such steps to secure the Data Breach or possible cyber security incident.

8.2.5. To the extent ONDC is required under Applicable Law~~,~~ it shall provide notice or information relating to the Data Breach to any Competent Authority or all affected parties.

8.3. Certification

[1]**Ecosystem Participant** shall mean any participant in the ONDC ecosystem other than Network Participants, and includes the Technology Service Providers, Sellers and other ONDC Network participants who may not have any direct contractual relationship with ONDC, but are engaged by the Network Participants in relation to activities carried out over the ONDC Network.

8.3.1. At the time of onboarding with the ONDC Network, the Network Participant must (i) comply with the Certification Process as stipulated in Chapter 1 of the Network Policy; and (ii) provide an undertaking that it will comply with the Applicable Laws, ONDC Network Policy and operational benchmarks once it has been onboarded in the ONDC Network.

8.3.2. After one year from the date of onboarding with the ONDC Network, the Network Participant shall on a yearly basis:

(a) provide a certificate in form of a report from an information systems auditor empanelled by ONDC or CertIn empanelled auditor certifying the: (i) reasonable security practices and procedures implemented by the Network Participant;

(b) provide ONDC an undertaking regarding its overall compliance and, if applicable, the compliance of the service providers engaged by such Network Participant, with the Network Policy as provided in Schedule 8A (**Annual Undertaking**), before three months from the date of completion of one year period or as extended at the sole discretion of ONDC. *For clarity*, the term 'service providers' in this clause shall not include Buyer Apps, Seller Apps and Gateways.

(c) Network Participant shall ensure, in the best of their efforts, that there is no/minimum disruption to any stakeholder of the ONDC Network due to any App deployment or App maintenance by the Network Participant.

8.4. Audit

8.4.1. In case of a cybersecurity incident, ONDC may audit the Network Participant's information and communication technology systems (ICT) related to ONDC operations, either by itself or through an auditor appointed by ONDC. ONDC will clearly communicate the purpose of such audits. The continuation of operations as a Network Participant shall, at all times, be dependent upon the said audit confirming the Network Participant's compliance with the requirement in question. Any failure in compliance of the same, if confirmed in the audit, may result in disciplinary action such as fines or suspension/termination of access to the ONDC Network.

8.4.2. It is clarified that ONDC will not audit entities in the financial services domain that are regulated by the Reserve Bank of India, the Securities and Exchange Board of India, or the Insurance Regulatory and Development Authority of India, such as lending institutions. However, ONDC may require these Network Participants to submit a summary report from a CERT-In empanelled auditor, only in relation to such Network Participant's ONDC operations.

8.4.3. ONDC shall provide a reasonable advance notice to the Network Participant to undertake the audit. However, ONDC may order an audit without any advance notice in case of an emergency, such as a major data breach, the commission of a major crime, or an incident that threatens the integrity of the ONDC Network. ONDC shall, in all cases, provide a reason for ordering the audit in the notice ordering/requiring it.

8.4.4. Network Participant must extend full cooperation and provide such explanation as may be required for the purpose of any inspection or audit authorised by the Competent Authority or other authorised official of ONDC regarding the Network Participant's non-compliance with the Applicable Law or the Network Policy.

DEFINITIONS

Certification Process means the validation report or certificate obtained from a third-party auditor or a certifying agency duly recognised by ONDC or by ONDC itself in relation to the Network Participant's compliance with the ONDC Protocol Specification.

Data Breach has the meaning ascribed to it in Clause 8.2.2.

Schedule 8A

I, a Network Participant of the ONDC Network, hereby declare that I am in compliance with all requirements under Applicable Law and in full compliance with ONDC Network Policy.

I further undertake that all service providers engaged by me for providing any service or product on the ONDC Network are also in compliance with this Network Policy to the extent applicable.

I understand that if any information is found to be false, ONDC reserves the right to take any other action as prescribed under the Network Policy, including the right to suspend my access to the ONDC Network, and take necessary recourse as applicable under the Applicable Law.

Version History

Version	Date	Description
0.3	3rd October 2022	Released to NPs
1.0	22nd October 2022	- Added "Applicable Laws" to Clause 8 - Clarified language on security standards in clause 8.1.2 - Harmonised the clause on minimum disruption with the uptime requirements in Chapter 2: Business Rules - Removed ambiguity in clause 8.3.2 regarding undertaking related to compliance by Ecosystem Participants - Removed obligation on recertification following a Major App Update - Added a notice requirement for ordering an audit, including a requirement to provide a reason for the audit - Fixed definitions section - Annexure amended to clarify that the undertaking has to be on behalf of service providers engaged by the Network Participant
2.0	15th February, 2024	Simplified and Rationalised Chapter released to NPs
2.1	05th December, 2024	- Simplified Security Breach Procedure in Clause 8.2.5 - Expanded Certification Options (Clause 8.3.2(a)): Network Participants can now provide a certificate from either an ONDC-empaneled auditor or a CERT-In empaneled auditor, offering greater flexibility in certification requirements - Clarified that audits by ONDC are limited to ICT systems related to ONDC operations - Clarified that audit of entities operating in financial services domain