XtraTrust DigiSign Private Limited

UIDAI Information Security Policy

Authentication User Agencies (AUAs) and KYC User Agencies (KUAs)

Version 1.0

1 Document Control Page

1.1. Revision History

Ver No.	Date	Prepared BY	Reviewed By	Approved By	Changes	Section/ Pages
1.0	05-11-2024	Arush Pawar	Krunal Pandya	Sameer Kumar	Initial Document	21
2.0						
3.0						

1.2. Policy Ownership and Review Frequency

SN	Ownership	Minimum Review Frequency	Last Reviewed	Remarks
1	CISO	Annually	05-11-2024	Initial Document
2	CISO	Annually	08-12-2024	Reviewed
3				
4				

Table of Contents

2 Purpose

The Information Security Policy for Authentication User Agencies (AUAs) and KYC User Agencies (KUAs) is an additional Information security Policy document to existing Information Technology and Security Policy document available at XtraTrust.

It is developed to ensure the secure handling, transmission, and storage of Aadhaar data. It aims to ensure robust IT security measures that align with the unique operational requirements of the UIDAI. It supports the XtraTrust's commitment to effective management and operational integrity, ensuring compliance with all regulatory and security standards.

3 Coverage

The Policies applies to:

- XtraTrust Officers (both main and DR site).
- Outsourced personnel at RCAI:

The Information Security Policies outlined in this document apply to all designated personnel responsible for the operation, maintenance, and security of the AUA/KUA operational environment. This includes:

- Individuals assigned, roles and responsibilities.
- All personnel involved in AUA/KUA activities.

These policies are specifically designed to address the unique requirements of the UIDAI's requirement as outlined in the broad overview below.

a) The term Site includes both the main site and its DR site, as well as their respective personnel.
b) Data sent is encrypted.
c) Continuous operations, CCTV, access control, and environmental systems, with premises accessed infrequently.
d) All operations require at least two personnel.
e) Roles are assigned based on specific activities with no role conflict allowed.
f) The passwords are securely stored and retrieved by two officers.
g) Security personnel guard the building for entry/exit verification.
h) For fire and water detection systems, alarms are installed

This document is subject to general XtraTrust Security Management Guidelines issued from time to time and Principles & Practices followed thereto. Where it fails to refer to specific issues, of IT Act, Rules, Regulation and Guidelines issued by O/o UIDAI from time to shall prevail.

4 Information Security Policy

The XtraTrust Information Security Policy is designed to govern the use of IT assets and functionalities within the XtraTrust environment.

These policies are intended to:

- Protect people and information;
- Set the rules for expected behavior by users, systems and administrators
- Focus on auditing and logging activities rather than network security/monitoring considering offline mode.
- Define roles for audit and log review following each operational session.
- Define and authorize the consequences of violation;
- Define the consensus baseline stance on security;
- Help minimize risk;
- Help track compliance with regulations and legislation;
- Ensuring that all XtraTrust officers are aware of and fully comply with the relevant legislation as described in this and other policies;
- Describing the principals of security and explaining how they shall be implemented in the organization;
- Introducing a consistent approach to security, ensuring that all XtraTrust officers fully understand their own responsibilities;
- Creating and maintaining within the RCAI a level of awareness of the need for IT Security as an integral part of the day to day business;
- Protecting information assets under the control of the RCAI.

4.1. Policy Enforcement

Any deliberate and / or serious breach of these policies will lead to disciplinary measures as stipulated in the Disciplinary Code of Practice of the XtraTrust.

The following formal meetings and/or communication forums will be established within XtraTrust in order to ensure the successful execution of the tasks regarding the implementation of this document.

- All new XtraTrust officers will be informed of the content of this policy and procedures during their orientation;
- The XtraTrust officers will be expected to sign that they understand the content thereof;
- The officers will sign to accept the actions that can be taken in the event of non-conformance to the policy and procedure;
- The officers will sign to accept the responsibilities regarding the policies and procedures on their area of operations;

- The officers will sign to accept the resultant actions that must be taken in the event that one of the policies has been breached;
- All Contractors and/or Temporary officers who require access to XtraTrust infrastructure will utilize IT Infrastructure will be bound by and must sign acceptance of the contents of this policy (Non-Disclosure Agreement (NDA) prior to commencement of their assignments;
- All Managed XtraTrust IT Services (outsourced) officers who require access to XtraTrust infrastructure or will utilize or manage IT Infrastructure on behalf of XtraTrust will be bound by and must sign acceptance of the contents of this policy Non-Disclosure Agreement (NDA) prior to commencement of their assignments;
    - It shall be noted that the XtraTrust Information Security reserves the right to audit internal networks and systems and external VPN connectivity between Main and DR site on a periodic basis to ensure compliance with this document.

4.2. Responsibilities

Ultimate accountability for Information Security rests with the CISO, but on a day-to-day basis the XtraTrust Information Security team shall be responsible for managing and implementing the policy and related procedures. CISO is responsible for the effective implementation, monitoring of Information security management system (ISMS) at XtraTrust.

Head of Department is responsible for ensuring that their permanent and temporary staff and CISO is aware of:

- The Information Security policies applicable in their work areas;
- Their personal responsibilities for Information Security;
- How to access advice on Information Security matters;

Individuals shall be responsible for the security of their physical environments where information is processed or stored.

All staff shall comply with Information Security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.

Each member of staff shall be responsible for the operational security of the information systems they use.

Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.

Contracts with external contractors that allow access to the organization's information systems shall be in operation before access is allowed. These contracts shall ensure that

the staff or sub-contractors of the external organization shall comply with all appropriate security policies.

4.3. Policies Maintenance and Updates

XtraTrust Officers shall ratify the entire Security Policy before it is implemented. As technology is dynamic, the security policy needs anon-going review to keep pace with threats arising out of the new technology. The policies shall be maintained, reviewed and updated by the CISO. This review shall take place at least once per annum.

5 Data Protection and Privacy

5.1.1 Objective

To create a robust defense mechanism to protect information security that would impact the confidentiality and integrity of data at XtraTrust.

5.1.2 Scope

This policy applies to all the controls applied to all systems, people, processes that constitute the organization's information management system, including top management, officers and suppliers and other third parties who have access to XtraTrust systems.

5.1.3 Policy

- **Secure Storage and Handling**: AUAs and KUAs must implement robust systems for securely storing and handling Aadhaar data, ensuring it's protected against unauthorized access and breaches.
- **Privacy Compliance**: Compliance with the Aadhaar Act and other privacy laws is mandatory. This involves ensuring that individual privacy rights are respected and protected in all data processing activities.

5.1.4 Compliance

The CISO will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

- **Non-Compliance**

Any Officer(s) found to have violated this policy may be subjected to disciplinary action.

- **Exceptions/ Deviations**

This policy shall take effect upon publication or release. If compliance with this policy is not feasible or technically not possible, or if deviation from this policy is necessary to support a function, inform CISO for a security exception.

6 Encryption and Data Security

6.1.1 Objective

To create a robust defence mechanism to protect information security that would impact the confidentiality and integrity of data at XtraTrust.

6.1.2 Scope

This policy applies to all the controls applied to all systems, people, processes that constitute the organization's information management system, including top management, officers and suppliers and other third parties who have access to XtraTrust systems.

6.1.3 Policy

To provide awareness of the threat to information security for XtraTrust officers for taking appropriate mitigation actions.

- **End-to-End Encryption**: Aadhaar data must be encrypted during transmission and storage. The policy specifies using advanced encryption standards to safeguard data.
- **Data Masking**: When displaying Aadhaar data, sensitive parts of the information should be masked to prevent unauthorized viewing.

6.1.4 Compliance

The CISO will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

- **Non-Compliance**

Any Officer(s) found to have violated this policy may be subjected to disciplinary action.

- **Exceptions/ Deviations**

This policy shall take effect upon publication or release. If compliance with this policy is not feasible or technically not possible, or if deviation from this policy is necessary to support a function, inform CISO for a security exception.

7 Access Control

7.1.1 Objective

To create a robust defense mechanism to protect information security that would impact the confidentiality, integrity and availability of data at XtraTrust.

7.1.2 Scope

This policy applies to all the controls applied to all systems, people, processes that constitute the organization's information management system, including top management, officers and suppliers and other third parties who have access to XtraTrust systems.

7.1.3 Policy

To provide awareness of the threat to information security for XtraTrust officers for taking appropriate mitigation actions.

- **User Access Management**: Implement strict access controls to restrict data access to authorized personnel only. This includes managing user identities, authentication, authorization, and audit trails.
- **Two-Factor Authentication**: Wherever possible, implement two-factor authentication for additional security.

7.1.4 Compliance

The CISO will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

- **Non-Compliance**

Any Officer(s) found to have violated this policy may be subjected to disciplinary action.

- **Exceptions/ Deviations**

This policy shall take effect upon publication or release. If compliance with this policy is not feasible or technically not possible, or if deviation from this policy is necessary to support a function, inform CISO for a security exception.

8 Audit and Compliance of UIDAI Information Security Policy

8.1.1 Objective

To create a robust defence mechanism to protect information security that would impact the confidentiality and integrity of data at XtraTrust by compliance to policy and verification through audit.

8.1.2 Scope

This policy applies to all the controls applied to all systems, people, processes that constitute the organization's information management system, including top management, officers and suppliers and other third parties who have access to XtraTrust systems.

8.1.3 Policy

To provide awareness of the threat to information security for XtraTrust officers for taking appropriate mitigation actions.

- **Regular Audits**: Conduct thorough and regular audits to assess compliance with UIDAI guidelines and identify potential security gaps.
- **Incident Reporting**: Any security incidents or breaches involving Aadhaar data must be promptly reported to UIDAI.

8.1.4 Compliance

The CISO will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

- **Non-Compliance**

Any Officer(s) found to have violated this policy may be subjected to disciplinary action.

- **Exceptions/ Deviations**

This policy shall take effect upon publication or release. If compliance with this policy is not feasible or technically not possible, or if deviation from this policy is necessary to support a function, inform CISO for a security exception.

9 Network Security

9.1.1 Objective

To create a robust defence mechanism to protect information security of networks used in XtraTrust and that would impact the confidentiality, integrity and availability of data at XtraTrust.

9.1.2 Scope

This policy applies to all the controls applied to all systems, people, processes that constitute the organization's information management system, including top management, officers and suppliers and other third parties who have access to XtraTrust systems.

9.1.3 Policy

To provide awareness of the threat to information security for XtraTrust officers for taking appropriate mitigation actions.

- **Network Infrastructure Security**: Secure network infrastructure to protect data in transit. This includes using secure VPNs, SSL/TLS, and other secure communication protocols.
- **Monitoring and Detection**: Continuous monitoring of network traffic and implementing intrusion detection systems to identify and respond to threats in real-time.

9.1.4 Compliance

The CISO will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

- **Non-Compliance**

Any Officer(s) found to have violated this policy may be subjected to disciplinary action.

- **Exceptions/ Deviations**

This policy shall take effect upon publication or release. If compliance with this policy is not feasible or technically not possible, or if deviation from this policy is necessary to support a function, inform CISO for a security exception.

10 Incident Management

10.1.1 Objective

To create a robust defence mechanism to protect information security that would impact the confidentiality and integrity of data at XtraTrust through managing incidents.

10.1.2 Scope

This policy applies to all the controls applied to all systems, people, processes that constitute the organization's information management system, including top management, officers and suppliers and other third parties who have access to XtraTrust systems.

10.1.3 Policy

To provide awareness of the threat to information security for XtraTrust officers for taking appropriate mitigation actions.

- **Incident Response Plan**: A well-defined incident response plan should be in place to handle data breaches or security incidents effectively and minimize impact.
- **Breach Notification**: In case of a breach, a protocol for notifying affected individuals and authorities in a timely manner is necessary.

10.1.4 Compliance

The CISO will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

- **Non-Compliance**

Any Officer(s) found to have violated this policy may be subjected to disciplinary action.

- **Exceptions/ Deviations**

This policy shall take effect upon publication or release. If compliance with this policy is not feasible or technically not possible, or if deviation from this policy is necessary to support a function, inform CISO for a security exception.

11 Data Retention and Disposal

11.1.1 Objective

To create a robust defence mechanism to protect information security that would impact the confidentiality, integrity and availability of data at XtraTrust in data stored and disposed.

11.1.2 Scope

This policy applies to all the controls applied to all systems, people, processes that constitute the organization's information management system, including top management, officers and suppliers and other third parties who have access to XtraTrust systems.

11.1.3 Policy

To provide awareness of the threat to information security for XtraTrust officers for taking appropriate mitigation actions.

- **Data Retention Policy**: Clear guidelines on how long Aadhaar data should be retained and under what circumstances it can be stored.
- **Secure Data Disposal**: Ensure that data is disposed of securely and is irretrievable once it is no longer needed.

11.1.4 Compliance

The CISO will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

- **Non-Compliance**

Any Officer(s) found to have violated this policy may be subjected to disciplinary action.

- **Exceptions/ Deviations**

This policy shall take effect upon publication or release. If compliance with this policy is not feasible or technically not possible, or if deviation from this policy is necessary to support a function, inform CISO for a security exception.

12 Employee Training and Awareness about UIDAI Information Security Policy

12.1.1 Objective

To create a robust defence mechanism to protect information security that would impact the confidentiality and integrity of data at XtraTrust through employee training.

12.1.2 Scope

This policy applies to all the controls applied to all systems, people, processes that constitute the organization's information management system, including top management, officers and suppliers and other third parties who have access to XtraTrust systems.

12.1.3 Policy

To provide awareness of the threat to information security for XtraTrust officers for taking appropriate mitigation actions.

- **Regular Training Programs**: Employees should receive regular training on data protection, privacy laws, and security best practices.
- **Security Awareness**: Creating a culture of security awareness within the organization is critical. This includes educating employees about phishing, social engineering, and other common cyber threats.

12.1.4 Compliance

The CISO will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

- **Non-Compliance**

Any Officer(s) found to have violated this policy may be subjected to disciplinary action.

- **Exceptions/ Deviations**

This policy shall take effect upon publication or release. If compliance with this policy is not feasible or technically not possible, or if deviation from this policy is necessary to support a function, inform CISO for a security exception.

13 Vendor and Third-Party Management

13.1.1 Objective

To create a robust defense mechanism to protect information security that would impact the confidentiality and integrity of data at XtraTrust through third party management and vendor management.

13.1.2 Scope

This policy applies to all the controls applied to all systems, people, processes that constitute the organization's information management system, including top management, officers and suppliers and other third parties who have access to XtraTrust systems.

13.1.3 Policy

To provide awareness of the threat to information security for XtraTrust officers for taking appropriate mitigation actions.

- **Vendor Security Requirements**: Vendors and third-party service providers must adhere to the same security standards as the AUA/KUA.
- **Vendor Audits**: Regular audits of vendors to ensure they are compliant with UIDAI's security requirements.

13.1.4 Compliance

The CISO will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

- **Non-Compliance**

Any Officer(s) found to have violated this policy may be subjected to disciplinary action.

- **Exceptions/ Deviations**

This policy shall take effect upon publication or release. If compliance with this policy is not feasible or technically not possible, or if deviation from this policy is necessary to support a function, inform CISO for a security exception.

14 Business Continuity and Disaster Recovery

14.1.1 Objective

To create a robust defence mechanism to protect information security that would impact the confidentiality and integrity of data at XtraTrust through business continuity and Disaster recovery management.

14.1.2 Scope

This policy applies to all the controls applied to all systems, people, processes that constitute the organization's information management system, including top management, officers and suppliers and other third parties who have access to XtraTrust systems.

14.1.3 Policy

To provide awareness of the threat to information security for XtraTrust officers for taking appropriate mitigation actions.

- **Disaster Recovery Planning**: Robust disaster recovery plans to ensure business continuity and data integrity in the event of a disaster.
- **Regular Testing**: Regular testing and updating of disaster recovery and business continuity plans to ensure they are effective and current.

14.1.4 Compliance

The CISO will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

- **Non-Compliance**

Any Officer(s) found to have violated this policy may be subjected to disciplinary action.

- **Exceptions/ Deviations**

This policy shall take effect upon publication or release. If compliance with this policy is not feasible or technically not possible, or if deviation from this policy is necessary to support a function, inform CISO for a security exception.

15 Legal and Regulatory Obligations of UIDAI Information Security Policy

15.1.1 Objective

To create a robust defence mechanism to protect information security that would impact the confidentiality and integrity of data at XtraTrust for meeting legal and regulatory obligations.

15.1.2 Scope

This policy applies to all the controls applied to all systems, people, processes that constitute the organization's information management system, including top management, officers and suppliers and other third parties who have access to XtraTrust systems.

15.1.3 Policy

To provide awareness of the threat to information security for XtraTrust officers for taking appropriate mitigation actions.

- **Regulatory Adherence**: Keeping abreast of and complying with all legal and regulatory changes pertaining to Aadhaar data and privacy laws.

- **Contractual Agreements**: Ensuring that contracts with partners, vendors, and third parties include clauses that bind them to the same level of data protection and privacy standards.

15.1.4 Compliance

The CISO will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

- **Non-Compliance**

Any Officer(s) found to have violated this policy may be subjected to disciplinary action.

- **Exceptions/ Deviations**

This policy shall take effect upon publication or release. If compliance with this policy is not feasible or technically not possible, or if deviation from this policy is necessary to support a function, inform CISO for a security exception.

16 Technology and Infrastructure Management

16.1.1 Objective

To implement a robust defence technology to protect information security of confidentiality and integrity of data at XtraTrust.

16.1.2 Scope

This policy applies to all the controls applied to all systems, people, processes that constitute the organization's information management system, including top management, officers and suppliers and other third parties who have access to XtraTrust systems.

16.1.3 Policy

To provide awareness of the threat to information security for XtraTrust officers for taking appropriate mitigation actions.

- **Infrastructure Security**: Secure infrastructure management, including regular updates and patch management to protect against vulnerabilities.

- **Data Integrity Measures**: Implementing measures to ensure the integrity of Aadhaar data, preventing corruption or alteration.

16.1.4 Compliance

The CISO will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

- **Non-Compliance**

Any Officer(s) found to have violated this policy may be subjected to disciplinary action.

- **Exceptions/ Deviations**

This policy shall take effect upon publication or release. If compliance with this policy is not feasible or technically not possible, or if deviation from this policy is necessary to support a function, inform CISO for a security exception.

17 Risk Management

17.1.1 Objective

To create a robust defence mechanism to protect information security that would impact the confidentiality and integrity of data at XtraTrust by implementing risk management.

17.1.2 Scope

This policy applies to all the controls applied to all systems, people, processes that constitute the organization's information management system, including top management, officers and suppliers and other third parties who have access to XtraTrust systems.

17.1.3 Policy

To provide awareness of the threat to information security for XtraTrust officers for taking appropriate mitigation actions.

- **Risk Assessment and Management**: Regular risk assessments to identify and manage potential risks associated with Aadhaar data handling and processing.
- **Change Management**: A well-structured change management process to ensure that any changes in systems or processes do not compromise data security.

17.1.4 Compliance

The CISO will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

- **Non-Compliance**

Any Officer(s) found to have violated this policy may be subjected to disciplinary action.

- **Exceptions/ Deviations**

This policy shall take effect upon publication or release. If compliance with this policy is not feasible or technically not possible, or if deviation from this policy is necessary to support a function, inform CISO for a security exception.