This document is not to be treated as a draft of the Regulations under the proposed National Identification and Registration Act. The document was formulated solely to act as an aid in the deliberations on the Report of the Joint Select Committee which considered the Bill shortly entitled the National Registration and Identification Act, 2020 by providing an example of the information likely to be inserted in the Regulations. The information in this document is based on the provisions in that Bill and the recommendations of the Joint Select Committee. The promulgated Regulations may differ significantly in content from this document as a result of changes which may be made to the principal legislation during the legislative process and will differ significantly in form as the Regulations to be promulgated will be the product of the Office of Parliamentary Counsel. This document does not have, nor is it intended to have legal effect.

NATIONAL IDENTIFICATION AND REGISTRATION ACT, 2021

NATIONAL DATABASES (DATA SECURITY) REGULATIONS, 2021

1. Short title and commencement. —

(1) These regulations may be called the National Identification and Registration (Data Security) Regulations, 2021.

(2) For the avoidance of doubt, these Regulations shall apply to the National Identification and Registration Authority, personnel, service providers, and accredited third parties.

2. **Interpretation**. -

(1) In these Regulations –

"accredited third party" means a person that submits the National Identification Number and identity information of an enrolled individual to the Authority for authentication or verification;

"the Act" means the National Identification and Registration Act, 2021;

"enrolment centre" means a place designated by the Authority for the purposes of these Regulations as a place where the enrolment of individuals may take place;

"enrolment agency" means an entity designated by the Authority to enrol individuals in the National Identification Databases;

"identity information" means the biographic, biometric or numerical references that may be collected by the Authority in respect of an enrolled individual;

"information security policy" means the policy specified by the Authority under regulation 3 of these regulations;

"National Identification Databases" means the databases in which all identity information collected under the Act by the Authority is stored;

"personnel" means all officers, employees, staff and other individuals employed or engaged by the Authority, enrolment agencies for discharging any functions under the Act;

"regulations" means the regulations made by the Authority under the Act;

"requesting person" means any person who, not being an accredited third party, submits the National Identification Number for authentication;

"service providers" includes all persons engaged by the Authority for discharging any function related to its processes.

(2) In accordance with section 12(2) of the Interpretation Act, expressions used in these Regulations that are defined in the Act have the same meanings assigned to them, respectively, in the Act, unless there is anything in the subject and context repugnant to or inconsistent with such meanings, respectively.

3. Measures for ensuring information security. —

(1) The Authority shall, from time to time, specify an information security policy setting out matters including the technical and organisational measures to be adopted by the Authority and its personnel, and also security measures to be adopted by agencies, advisors, consultants and other service providers engaged by the Authority, accredited third parties and persons to whom identity information may be disclosed.

(2) Such information security policy may provide for: —

(a) identifying and maintaining an inventory of assets associated with the information and information processing facilities;

(b) implementing controls to prevent and detect any loss, damage, theft or compromise of the assets;

(c) allowing only controlled access to confidential information;

(d) implementing controls to detect and protect against virus/malwares;

(e) a change management process to ensure information security is maintained during changes;

(f) a patch management process to protect information systems from vulnerabilities and security risks;

(g) a robust monitoring process to identify unusual events and patterns that could impact security and performance of information systems and a proper reporting

and mitigation process;
(h) encryption of data packets containing biometrics, and enabling decryption only in secured locations;
(i) partitioning of the National Databases network into zones based on risk and trust;
(j) deploying necessary technical controls for protecting the National Databases network;
(k) service continuity in case of a disaster;
(l) monitoring of equipment, systems and networks;
(m) measures for fraud prevention and effective remedies in case of fraud;
(n) requirement of entering into non-disclosure agreements with the personnel;
(o) provisions for audit of internal systems and networks;
(p) restrictions on personnel relating to processes, systems and networks;
(q) processes for the disposal of information systems assets and any computer media;
(r) inclusion of security and confidentiality obligations in the agreements or arrangements with the agencies, consultants, advisors or other persons engaged by the Authority.
(3) The Authority shall monitor compliance with the information security policy and other security requirements through internal audits or through independent agencies.
(4) The Authority shall designate an officer as Chief Information Security Officer for disseminating and monitoring the information security policy and other security-related programmes and initiatives of the Authority including incident reporting in accordance with the information security policy.

4. Security obligations of personnel —
(1) The personnel shall comply with the information security policy, and other policies, guidelines, procedures, etc. issued by the Authority from time to time.
(2) Without prejudice to any action that may be taken under the Act, personnel may be liable to action in accordance with procedures specified by the Authority for this purpose: Provided that no such action shall be taken without giving the concerned personnel a reasonable opportunity of being heard.

5. Security obligations of enrolment agencies, consultants, service providers, etc. —
The agencies, consultants, advisors, accredited third parties and service providers engaged by the Authority for discharging any function relating to its processes shall:
(a) ensure compliance with the information security policy specified by the Authority;
(b) periodically report compliance with the information security policy and contractual requirements, as required by the Authority;
(c) report promptly to the Authority any security incidents affecting the confidentiality, integrity and availability of information related to the Authority's functions;
(d) ensure that records related to the Authority shall be protected from loss, destruction, falsification, unauthorised access and unauthorised release;

(e) ensure confidentiality obligations are maintained during the term and on termination of the agreement;

(f) ensure that appropriate security and confidentiality obligations are provided for in their agreements with their employees and staff members;

(g) ensure that the employees having physical access to the National Identification Databases data centres and logical access to National Identification Databases data centres undergo necessary background checks;

(h) define the security perimeters holding sensitive information, and ensure only authorised individuals are allowed access to such areas to prevent any data leakage or misuse; and

(i) where they are involved in the handling of the biometric data, ensure that they use only those biometric devices which are certified by a certification body as identified by the Authority and ensure that appropriate systems are built to ensure security of the biometric data.

6. Audits and inspection of service providers, etc. —

(1) All agencies, consultants, advisors and other service providers engaged by the Authority, and accredited third parties shall get their operations audited in accordance with the standards utilised by the Authority and furnish certified audit reports to the Authority, upon request or at time periods specified by the Authority.

(2) In addition to the audits referred to in sub-regulation (1), the Authority may conduct audits of the operations and systems of such entities or persons, either by itself or through an auditor appointed by the Authority.

7. Confidentiality. –

All procedures, orders, processes, standards and protocols related to security, which are designated as confidential by the Authority, shall be treated as confidential by all its personnel and shall be disclosed to the concerned parties only to the extent required for giving effect to the security measures.

8. Power to issue policies, processes, documents, etc. —

The Authority may issue policies, processes, standards and other documents, not inconsistent with these regulations, which are required to be specified under these regulations or for which provision is necessary for the purpose of giving effect to these regulations.

10. Power to issue clarifications, guidelines and removal of difficulties. —

In order to clarify any matter pertaining to application or interpretation of these regulations, or to remove any difficulties in implementation of these regulations, the Authority shall have the power to issue clarifications and guidelines in the form of circulars which shall have the effect of these regulations.

11. Security Standards

The Authority shall operate in accordance with internationally accepted best practices and standards of information and data security.