INFORMATION SECURITY POLICY

DVARA KSHTERIYA GRAMIN FINANCIAL SERVICES PRIVATE LIMITED	
Policy	**Information Security Policy**
Version	**7.0**
Date of approval by Board	**May 05, 2019**
Date of Last Review by Board	**August 14, 2025**
Process Owner	**Chief Information Security Officer**

Department	Information Security
Document Reviewer	Kasiviswanathan S
Document Approver	Board
Document Classification	**Internal**
Document Status	**Final**

Revision History

Version No.	Date	Description	Change Mode (A/M/D/NC) A - Added/M - Modified/D - Deleted/NC - No Change	Change Made By	Reviewed on	Approved on
V 6.0	11/09/23	V5.0 is compressed with policy details only	M	Kasi Viswanathan	13/09/23	14/02/2024
V 7.0	NA	Review and update	M	Kasi Viswanathan	NA	05/03/2025
V 8	23/07/25	Minor updates	M	Sabareeshwaran	24/07/25	14/08/2025

Release no.	Release date	Change details
1.0	05-May-2019	First Release
2.0	31-Mar-2021	Second Release
3.0	17-Jul-2021	Third Release
4.0	02-Nov-2022	Fourth Release
5.0	08-Aug-2023	Fifth Release
6.0	14-Feb-2024	Sixth Release
7.0	05-Mar-2025	Seventh Release
8.0	14-Aug-2025	Eight Release

1. Introduction

Information security is a holistic discipline, meaning that its application, or lack thereof, affects all facets of an organization or enterprise. The goal of the Dvara KGFS Information Security Program is to protect the Confidentiality, Integrity, and Availability of the data employed within the organization while providing value to the way we conduct business. Protection of the Confidentiality, Integrity, and Availability are basic principles of information security, and can be defined as:

1.1. Confidentiality – Ensuring that information is accessible only to those entities that are authorized to. have access, many times enforced by the classic “need-to-know” principle.

1.2. Integrity - Protecting the accuracy and completeness of information and the methods used to process and manage it.

1.3. Availability – Ensuring that information assets (information, systems, facilities, networks, and computers) are accessible and usable when needed by an authorized entity.

Dvara KGFS has recognized that business information is a critical asset and as such the ability to manage, control, and protect this asset will have a direct and significant impact on its future success.

This document establishes the policy from which other information security processes may be developed to ensure that the enterprise can efficiently and effectively manage, control, and protect its business information assets and those information assets entrusted to Dvara KGFS by its stakeholders, partners, customers and other third parties.

The Dvara KGFS Information Security Program is built around the information contained within this policy and its supporting policies.

2. Objective

Dvara KGFS will review continually the internal and external factors that influence its ability to deliver its business objectives. Stakeholder expectations for information security would be evaluated to determine the scope for the Information Security policy and Information Security Management System, in compliance with applicable Regulators' directions thereof. Dvara KGFS shall identify and prioritize stakeholder needs and comply with required Regulators' guidelines and ensure measures that address information security risks, while ensuring continual improvement. The primary objectives of establishing Dvara KGFS's Information Security policy and Information Security Management System are:

- To maintain risks to Dvara KGFS' s enterprise information at an acceptable level and protect information against unauthorized disclosure, unauthorized or inadvertent modifications, and cybersecurity and internal threats and exposures.
- To ensure compliance with all applicable legal, statutory, regulatory and contractual provisions.
- To establish responsibility and accountability for information security in the organization.
- To encourage management and staff to maintain an appropriate level of awareness, knowledge and skills so as to minimize information security incidents.

3. Scope & Applicability

The Information Security policy covers all information pertaining to Dvara KGFS's line of businesses, including support functions like human resources, administration and IT operations, while meeting the statutory and regulatory requirements. This policy also covers all Information Technology Environments operated by an external entity or contracted with a third party.

This policy applies to all Dvara KGFS business units of information assets including its employees, vendors, business partners, contractor personnel and functions.

The term "Information Technology Environment" defines the total environment and includes, but is not limited to, all documentation, physical and logical controls, personnel, hardware, IT (Information Technology) equipment, software, services, and information. The Information Security Committee (ISC) or Board shall resolve any conflicts arising from this policy.

4. Terms & Definitions

Terms	Definitions
Asset	An application, general support system, high impact program, physical hardware, mission critical system, personnel, or a logically related group of systems which has a value to the organization.
Information	Data that has been organized, processed, or structured in a meaningful way to provide context, relevance, and value to a user.
Information Resources	Refer to the various types of data, content, and materials that organizations, entities, and personnel use to gather, create, store, and disseminate information
Security	A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions. despite risks posed by threats to its use of information systems.
Policy	Statements, rules or assertions that specify the correct or expected behavior of an entity.
Stakeholder	Individual or an entity having a right, share, claim, or interest in a system or in its possession of characteristics that meet their needs and expectations.
Standard	A published statement on a topic specifying characteristics, usually measurable, that must be satisfied or achieved in order to comply with the specified regulations and requirements.
Regulators	An Entity who is responsible for overseeing and enforcing rules, regulations, laws, standards, and compliance in specific industries or sectors. For Dvara KGFS, SEBI, RBI, IRDA & UIDAI are the main regulators.
Framework	is a structured and organized set of concepts, practices, guidelines, and tools that provide a foundation for developing, building, or solving complex problems within a specific vertical or context.

5. Policy Statement

Dvara KGFS maintains and communicates an Information Security Program consisting of topic-specific policies, standards, procedures, and guidelines, reflecting its commitment to safeguarding the confidentiality, integrity, and availability of business information including sensitive customer information.

The management and all employees/users at Dvara KGFS are committed to an effective system that:

- ✓ Supports its strategic business objectives and protects against information and cybersecurity threats and exposures.
- ✓ Serve to protect the Confidentiality, Integrity, and Availability of the Information Resources maintained within the organization using administrative, physical, and technical controls.
- ✓ Provide value to the way Dvara KGFS conduct business and support institutional objectives.
- ✓ DVARA KGFS shall ensure that all software development activities, whether conducted in-house or outsourced, adhere to secure coding practices. DVARA KGFS secure coding standards shall be periodically reviewed and updated in order to align with the CERT-In and regulatory guidelines. Comply with applicable regulatory and legal requirements, including:
    - Information Security best practices, including ISO 27001:2022
    - RBI cyber security framework
    - IRDAI Information and Cyber Security Guidelines,2023
    - SEBI Cyber Security & Cyber Resilience Framework
    - UIDAI Information Security guidelines

To achieve these goals, Dvara KGFS will:

- ✓ Continuously enhance the Information Security System by establishing and regularly monitoring measurable security objectives.
- ✓ Develop, implement, test, and maintain a Business Continuity Plan tailored to the nature of its business operations.
- ✓ Ensure clear communication of relevant security policies to customers, employees, and other stakeholders as applicable.

This policy statement shall apply to all employees and users of Dvara KGFS's information processing facilities. The Senior Management shall ensure that this policy is implemented, communicated, monitored and maintained at all levels of the organization and regularly reviewed for compliance and continual improvement.

6. Organizational structure

i. IT Strategy Committee (ITSC)

The direction and overall governance oversight is entrusted to the IT Strategy Committee (ITSC), that comprises of:

- Minimum of three directors as members.
- Director/Chairperson of the ITSC, who shall be an independent director and have substantial IT expertise in managing/ guiding information technology initiatives; and
- Members are technically competent

Dvara KGFS shall appoint a sufficiently senior level, technically competent and experienced in IT related aspects as Head of IT Function i.e., Chief Information Officer (CIO).

Under the oversight of the IT Strategy Committee, an Information Security Committee (ISC) shall be constituted, comprising of the Chief Information Security Officer and other representatives from the business and information technology functions as determined by the IT Strategy Committee. The ISC shall be headed by appropriate personnel from the risk management vertical.

Constitution of ISC should be as follows –

- Chief Information Security Officer (CISO)
- Representatives from business (decided by the IT Strategy Committee)
- Representatives from IT Function (decided by the IT Strategy Committee)
- The head of the ISC shall be from the risk management vertical.

ii. Roles and Responsibilities of relevant stakeholders

Roles	Responsibilities
IT Strategy Committee	• Approve information security program, policies and processes aligned with business of Dvara KGFS and encourage continual improvement. • Provide direction, support, and oversight for information security initiatives.

Information Security Committee	• Development of information/cyber security policies, implementation of policies, standards and procedures to ensure that all identified risks are managed within Dvara KGFS's risk appetite. • Approving/monitoring security projects and awareness initiatives • Reviewing information/cyber security incidents, information systems audit observations, monitoring and mitigating activities • Updating ITSC and CEO periodically on the activities of ISC
Top Management	• Ensure that an appropriate risk-based Information Security Program is implemented to protect the confidentiality, integrity, and availability of all Information Resources collected or maintained by or on behalf of Dvara KGFS. • Ensure that information security processes are integrated with the strategic and operational planning processes to secure the organization's mission. • Ensure adequate information security financial and personnel resources are included in the budgeting and/or financial planning process. • Ensure that the Security Team is given the necessary authority to secure the Information Resources under their control within the scope of the Dvara KGFS Information Security Program. • Designate an Information Security Officer and delegate authority to that individual to ensure compliance with applicable information security requirements. • Ensure that the Information Security Officer, in coordination with the Security Team, reports periodically to Executive.
Chief Information Security Officer (CISO)	• Chair the Security Team and provide updates on the status of the Information Security Program to Executive Management, including any remedial actions taken. • Place a review of cybersecurity risks/arrangements/preparedness of the RE before the Board/RMCB/ITSC at least on a quarterly basis and attend ITSC and IT Steering Committee meetings as a permanent invitee. • Manage compliance with all relevant statutory, regulatory, and contractual requirements and drive cyber security strategy and ensuring compliance to regulatory requirements. • Participate in security related forums, associations, and special interest groups.

	• Assess risks to confidentiality, integrity, and availability of all Information Resources collected or maintained by or on behalf of Dvara KGFS and develop and implement a process for evaluating risks related to vendors and managing vendor relationships. • Facilitate development and adoption of supporting policies, procedures, standards, and guidelines for providing adequate information security and continuity of operations. • Ensure that Dvara KGFS has trained all personnel to support compliance with information security policies, processes, standards, and guidelines, including contractors, and train and oversee personnel with significant responsibilities for information security with respect to such responsibilities. • Maintain a process for planning, implementing, evaluating, and documenting remedial actions to address deficiencies in information security policies, procedures, and practices, and develop and implement procedures for testing and evaluating the effectiveness of the Information Security Program in line with stated objectives. • Coordinate information/ cybersecurity related issues within the organization as well as with relevant external agencies
Chief Information Officer (CIO)	• Ensure that the execution of IT projects is aligned with the Dvara KGFS's IT Policy and IT Strategy. • Ensure effective organization structure that supports the IT functions

	of the Dvara KGFS. • Put in place an effective disaster recovery setup and business continuity strategy/plan. • Act as a first line of defense, ensuring effective assessment, evaluation and management of IT risk including the implementation of robust internal controls to secure the Dvara KGFS's information/IT assets. • Comply with extant internal policies, regulatory and legal requirements on IT related aspects.
Information Security Team	• Ensure compliance with applicable information security requirements. • Approve supporting procedures, standards, and guidelines related to information security. • Assess the adequacy and effectiveness of the information security policies and coordinate the implementation of information security controls. • Ensure that ongoing security activities are executed in compliance with policy.

	• Review and manage the information security policy waiver request process. • Review information security incident information and recommend follow- up actions. • Promote information security education, training, and awareness throughout Dvara KGFS, and initiate plans and programs to maintain information security awareness. • Report periodically, in coordination with the Security Officer, to Executive Management on the effectiveness of the Dvara KGFS Information Security Program, including progress of remedial actions. • Manage and monitor Security Operations Centre (SOC) and drive security related projects. • Ensure effective functioning of the security solutions deployed
Compliance Team	• Track changes to applicable regulations currently followed by the company. • Verify the applicability of newly introduced regulations. • Inform relevant stakeholders of any changes that need to be implemented to ensure compliance and prevent non-compliance.
Risk Management Team	• Identify internal and external risks across all lines of business with respect to, but not restricted to, information and cyber security. • Formulate measures for risk mitigation including systems and processes for internal control of identified risks.
Internal Audit teams	• Audit the implementation of this policy to ensure adequate coverage of IT/Technology infrastructure and applications. • Challenge the design and operating effectiveness of security controls to ensure effective and efficient information security system. • Conduct audit for third party /vendors handling critical data on planned and ad hoc basis to measure the effectiveness of the third-party
	security controls implemented. • Communicate and discuss with relevant line management and CISO for all instances of non-compliance related to Information security.
All Employees, Contractors, and Other Third-Party Personnel	• Understand each of their responsibilities for complying with the Dvara KGFS Information Security Program. • Use Dvara KGFS Information Resources in compliance with all Dvara KGFS Information Security Policies. • Seek guidance from Dvara KGFS Information Security Team for clarifications or issues related to information security practices/policies

7. Compliance

7.1. Compliance Measurement

Compliance Metrics will be derived based on the risk indicators and performance indicators identified from supportive information security procedures & process. The same would be reported to the appropriate Information Security Committee periodically for their attention and recommendations.

7.2. Exceptions

Any exception to this policy shall be approved by the CISO/ delegates.

8. Enforcement

Personnel found to have violated this policy may be subject to disciplinary actions, including but not limited to termination from employment. Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions at the discretion of Dvara KGFS.

9. Related Standards, Policies & Procedures

S. No	Standards, Policies & Procedures
1.	ISO 27001:2022 A 5.1,5.2
2.	RBI - Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices i. Para 24 (a), (b) [(i) (ii) (iii) (iv)], (d) [(i) (ii) (iii) (iv) (v) (vii)]

10. Review

The information security policy is reviewed no less than annually or upon significant changes to the information security environment.