CHRYSCAPITAL

Information Security Policy

Release date	12 December 2025
Prepared by	ChrysCapital Virtual CISO
Distribution	All Employees and Partners
Reviewed by	Ishaan Puri

Amendment Sheet			
Sr. No.	Date	Revision Status	Reason for Amendment
1.	12 December 2025	Initial Release	NA

I. Information Security:

1.1 Introduction:

Security of information and associated assets of ChrysCapital and the entities within its structure including but not limited to subsidiaries, affiliates, investment managers and funds (hereafter referred to as ChrysCapital), is of paramount importance. ChrysCapital shall endeavor to maintain the confidentiality, integrity and availability of its information and associated assets by identifying, deploying & operating controls that are proportionate to the criticality of the asset and protect the assets from all type of threats, whether internal or external, deliberate, or accidental.

The SEBI Cybersecurity and Cyber Resilience Framework (CSCRF) has been followed in this policy to ensure implementation of consistent cybersecurity guidelines and bolster the response to cyber risks, threats, and incidents. The principle in this policy is guided by ISO 27001:2022 to achieve implementation of industry best practices in ChrysCapital. Furthermore, ChrysCapital shall ensure that all legal, regulatory, statutory, and contractual obligations, as applicable, are met.

1.2 Policy Scope:

The policy shall be applicable to ChrysCapital and extends to all entities within its structure, including but not limited to subsidiaries, affiliates, investment managers and funds. (hereafter referred to as 'ChrysCapital')

Further, this policy applies to all employees, contractors, third-party vendors, and any other individuals that access or handle the ChrysCapital's information systems, networks, and data. The policy covers all organizational assets, including but not limited to:

a) Information systems, networks, applications, and databases.

b) All forms of data, including personal, confidential, and sensitive data.

c) Physical and virtual IT infrastructure, including cloud environments.

d) End-user devices such as desktops, laptops, mobile devices, and removable media.

The policy also applies to all locations, environments including on-premises facilities, remote work environments, and any third-party platforms or services used by the organization, ad includes, but is not limited to, all documentation, physical and logical controls, personnel, hardware, IT equipment, software, and information.

1.3 Policy statement:

ChrysCapital shall ensure protection of information, safety of its people and continuity of its business operations from key threats identified, whether internal or external, deliberate or accidental, such that the brand is protected; confidentiality of information is maintained; integrity of information can be relied upon and availability of information is ensured; in order to support business and meet customer expectations, while abiding to legal, regulatory and contractual obligations, by developing, implementing and continually improving information security management system.

1.4 Policy Objectives:

This policy provides management directive for information security and recommends appropriate security controls that need to be implemented to maintain and manage the information security in ChrysCapital. ChrysCapital shall secure information by: -

a) Creating and maintaining a security culture in ChrysCapital.

b) Ensuring compliance with all legal, regulatory, statutory, and contractual requirements.

c) Encouraging management and staff to maintain an appropriate level of awareness, knowledge, and skill to allow them to minimize the occurrence and severity of information security incidents.

d) Taking appropriate actions for any violations of the information security policy.

1.5 Roles and Responsibilities:

All the employees shall have the responsibility to read, understand and adhere to the information security policy. Users shall be responsible/accountable for actions associated with their use of information assets. They shall ensure that ChrysCapital information is not utilized for own personal gain and disclosing company information to unauthorized parties.

The third party/vendors shall have the responsibility to understand the ChrysCapital information security policy.

1.6 Review and Evaluation:

To ensure the effectiveness and relevance of the information security policy, it shall be reviewed and updated regularly. ChrysCapital shall conduct audits and inspections of its IT resources to check adherence with regulatory guidelines and standard industry practices, constitute an IT committee to review implementation of information security policy. The committee shall conduct the review on a periodic basis. The policy review will be conducted:

a) Annually, or more frequently if required by changes in the regulatory landscape, industry best practices, or new cybersecurity threats.

b) Following significant cybersecurity incidents to incorporate lessons learned and improve the organization's response to future incidents.

c) Upon implementation of new technologies or changes in business operations that impact the organization's security posture.

d) The review shall include, but not limited to:

   i) Feedback from business users.

   ii) Change in the business.

   iii) Change in the IT environment.

   iv) Change in the threat landscape.

   v) Reported security incidents.

e) All updates and revisions to this policy shall be communicated to relevant stakeholders, and necessary training or awareness programs will be conducted to ensure continued compliance.

1.7 Exception Handling:

Exception management controls the lifecycle of all the exceptions by a standardized method for efficient handling of all the exceptions. The policy is intended to be a statement of information and cybersecurity requirements that need to be met in ChrysCapital. As per the exception process:

a) IT personnel shall be responsible for enforcement of exception.

b) Exception shall be submitted using exception request form and sent to the Virtual CISO for processing, exceptions shall be valid for 180 days and will be reviewed by the Virtual CISO to determine whether the exception is still needed.

c) Approval shall be provided by the respective functional heads, evaluating all the risks, and then reviewed by Virtual CISO.

d) An approval matrix and exception management form shall be maintained.

e) All exceptions shall be centrally tracked and reviewed at least bi-annually by the Virtual CISO and be reported to the IT Committee.

Refer: Exception Request Form

II. Organization Control:

2.1 Policies for Information Security:

ChrysCapital shall ensure that its information security management system (ISMS) is consistently aligned with business objectives and remains robust against evolving security risks by establishing, implementing, and maintaining topic specific policies.

Implementation

a) Comprehensive information security and topic-specific policies shall be developed that cover all critical aspects of information security relevant to the organization.

b) Virtual CISO shall assess, identify, and reduce cybersecurity risks, respond to incidents, establish, and implement controls for cybersecurity and implementation of cyber resilience policy.

c) Communicate the policies effectively to all employees and relevant stakeholders through established procedure.

d) Adequate percentage of total IT budget to cybersecurity shall be allocated. Such allocation shall be mentioned under separate budgetary head for monitoring by the IT Committee members.

2.2 Information Security Roles and Responsibilities:

IT Committee of ChrysCapital shall provide direction and necessary support for implementation and maintenance of management system to ensure information security is in line with the defined policy.

General Partners	General Partners will provide direction and oversight the associated information and cybersecurity risks.
Information Technology Committee (IT)	IT Committee will seek regular updates on information security with ChrysCapital, review the associated risks and approve relevant policies and processes.
Information Security Working Group (ISWG)	Working Group will coordinate and ensure implementation of information and cybersecurity initiatives on an ongoing basis.

Implementation

a) Security responsibilities to individuals or teams based on their expertise shall be assigned.

b) Roles and responsibilities to all relevant stakeholders shall be communicated.

Refer-ChrysCapital-ISMS-Governance Structure V1.1

2.3 Segregation of Duties:

ChrysCapital shall ensure the segregation of conflicting duties and responsibilities, minimizing the potential for fraud, errors, and unauthorized activities.

a) An organizational structure such as defining roles, responsibilities, and reporting lines related to information security shall be established.

b) Clear reporting lines to prevent any individual from overseeing all key aspects of a process shall be defined.

c) IT Committee shall ensure the protection of information assets and maintain the integrity, availability, and confidentiality of the organization.

Refer-ChrysCapital-ISMS-Governance Structure V1.1

2.5 Contact with Authorities and Special Interest Groups:

Contact with law enforcement authorities, fire department, emergency services shall be maintained by the administration function. The contact details of these agencies shall be maintained and displayed at appropriate places.

The IT personnel shall maintain appropriate contact with special interest groups and authorized information security forums for receiving and distributing the updates on vulnerabilities, security threats, regulations and/or risks pertaining to the IT environment.

Implementation

a) The organization shall establish and maintain appropriate contact with relevant authorities, special interest groups, security forums to ensure compliance with applicable laws.

b) This includes opportunities to engage with relevant organizations for the purpose of professional education, seminars and networking events, promoting continuous improvement, and staying informed on industry trends and leading practices.

2.6 Asset and User End Point Devices Management:

ChrysCapital shall ensure that an accurate and comprehensive inventory of all information and associated assets, including their designated owners is developed and maintained to support effective asset management and security. Ensure that information stored on, processed by, or accessible via user endpoint devices is safeguarded against loss, theft, unauthorized access, and other forms of compromise.

Refer-ChrysCapital-ISMS-Asset Management and Media Disposal Process V1

2.7 Acceptable use of Information and Other Information Assets:

All employees shall have a responsibility for safeguarding all proprietary information, which includes but is not restricted to sensitive documents and information, from disclosure to unauthorized parties.

Implementation

a) The employee shall take due care and necessary approvals while disposing off/destroying confidential information.

b) Disruptions to network communication and security breaches are strictly prohibited.

Refer-ChrysCapital-ISMS-Acceptable usage policy V1

2.8 Classification and Labeling of Information:

Assets containing information useful to the organization shall be classified based on their relative business value, legal requirements, and impact due to loss of confidentiality, availability, and integrity of the information asset.

Implementation

The information assets shall be classified in the following four categories:

a) Public: Information freely available to the Public, all employees, and Partner(s). This type of information will not result any damage to ChrysCapital if it becomes generally known. There are no limitations on public information regarding creation, distribution, storing, disposal etc.

b) Internal: Information that is not meant for public consumption, however, can be shared with employees and Partner(s) for business related purposes. Internal information can be shared within ChrysCapital employees who have signed confidentiality clauses.

c) Confidential: Sensitive, strategic business information that could cause harm if shared inappropriately. Can be shared amongst a few groups of personnel only e.g., specific team, only managers and above etc. If unauthorized people gain access to company confidential information, this may lead to some financial, reputational, or other damage.

d) Strictly Confidential: Highly sensitive information, requiring the strictest protection where

usage is restricted within specific personnel only on a need-to-know basis. Restricted information includes but not limited to, trade secrets, sensitive personally identifiable information (PII), financial data, contracts, ChrysCapital intellectual properties, research and investor related information etc. If disclosed, there would be a significant financial, reputational, or legal impact to the business.

Refer-ChrysCapital-ISMS-Asset Management and Media Disposal Process V1

2.9 Access Management:

Access to ChrysCapital information systems shall be controlled in accordance with the business requirement, with subject to the principles of least privilege, segregation of duty and information security considerations.

ChrysCapital shall ensure secure handling of authentication information, access rights, and control the secure transfer of data while implementing strict identity and access management controls.

Implementation

a) Access shall be periodically reviewed and revoked when no longer necessary, such as in cases of employee termination or role changes.

b) Access control procedures shall be enforced that adhere to the principle of least privilege.

Refer-ChrysCapital-ISMS-User Access Management Procedure V1

2.10 Managing Information Security in the Information and Communication Technology (ICT) Supply Chain:

ChrysCapital shall ensure that all information security risks associated with ICT products and services in the supply chain are effectively managed.

Implementation

a) All ICT products and services that are sourced through third parties shall be identified.

b) It shall be ensured that all contracts and agreements with ICT suppliers include specific information security requirements.

Refer-ChrysCapital-ISMS-Asset Management and Media Disposal Process V1
Refer-ChrysCapital-ISMS-Third Party Risk Management Process V1

2.11 Information Security for Use of Cloud Services:

ChrysCapital shall ensure that the acquisition, use, management, and termination of cloud services aligns with the organization's information security requirements. This includes selecting cloud service providers (CSPs) based on security performance and ensuring secure migration or termination to minimize risks while maintaining data confidentiality, integrity, and availability.

Implementation

a) All security requirements related to cloud services shall be defined, including data protection, encryption, and incident management.

Refer-ChrysCapital-ISMS-Cloud Security Process V1

2.12 Privacy and Protection of Personal Identifiable Information (PII):

ChrysCapital shall identify and meet all applicable legal, regulatory, and contractual requirements for the privacy and protection of Personally Identifiable Information (PII). This involves implementing appropriate procedures and measures to safeguard PII in compliance with relevant privacy legislation, as applicable and ensuring that all relevant stakeholders are aware of their roles and responsibilities in protecting PII.

Refer-ChrysCapital-ISMS-Data Privacy Policy V1

2.13 Independent Review of Information Security:

ChrysCapital shall conduct independent reviews at planned intervals or whenever significant changes occur in the organization, such as changes in laws, introduction of new products or services, or significant incidents. Additionally, it shall be ensured that all relevant stakeholders comply with the organization's policies and to continuously measure the effectiveness of the ISMS, including implementing key performance indicators (KPIs).

2.14 Documented Operating Procedures:

The documentation shall be prepared for any operational activities that impact information security, ensuring that procedures are clear, comprehensive, and regularly updated. The objective is to ensure that operating procedures for information processing facilities are properly documented and made accessible to personnel who need them.

III. People Control:

3.1 Remote Working:

ChrysCapital shall ensure the security of sensitive information accessed, processed, or stored by personnel working remotely by implementing robust security measures that protect against unauthorized access and breaches.

Implementation

a) Types of work, data, and systems which can be accessed remotely shall be defined.

b) Remote workers shall be equipped with approved devices integrated with security tools.

Refer-ChrysCapital-ISMS-Acceptable Usage Policy V1

3.2 Human Resource Security:

ChrysCapital shall ensure that all personnel are held accountable for maintaining information security throughout their employment lifecycle. This includes background verification, defining terms and conditions of employment, conducting regular security awareness training, and enforcing disciplinary measures for violations of security policies, even after termination or role changes.

Implementation

a) Check on qualifications, identity, and references shall be conducted before employment.

b) Compliance with privacy and data protection laws shall be ensured during verification processes.

Refer-ChrysCapital-Policy Handbook V1

IV. Physical Security Control:

4.1 Physical Security Perimeters:

ChrysCapital shall establish comprehensive physical security measures which include secure physical perimeters, implement access control mechanisms, and ensure the security of offices, rooms, and facilities.

Implementation

a) Physical access attempts shall be logged through either physical logbooks or electronic systems.

b) Physical barriers such as secure gates shall be installed to prevent unauthorized access to facilities.

Refer-ChrysCapital-ISMS-Physical Security Process V1

4.2 Clear Desk and Clear Screen:

ChrysCapital shall ensure that sensitive or critical business information, whether in paper or electronic form, is securely stored when not in use and not accessible to unauthorized individuals. This includes preventing the loss, damage, or unauthorized access to information during and after business hours, ensuring that endpoint devices and digital displays are secured when unattended.

Implementation

a) Key locks or other physical security measures shall be used to secure endpoint devices (e.g., laptops, desktops) when left unattended or not in use.

b) It shall be ensured that all endpoint devices are logged off or have screen and keyboard locking mechanisms when unattended.

Refer-ChrysCapital-ISMS-Acceptable Usage Policy V1

4.3 Media Disposal:

ChrysCapital shall ensure that storage media containing sensitive information, along with supporting utilities and equipment, are securely managed, maintained, and disposed of. This includes preventing unauthorized access, mitigating environmental risks, and ensuring that sensitive data is securely erased before disposal or reuse.

Refer-ChrysCapital-ISMS-Asset Management and Media Disposal Process V1
Refer-ChrysCapital-ISMS-Physical Security Process V1

V. Technological Control:

5.1 Password Management

ChrysCapital shall ensure that secure and robust authentication methods are used to prevent unauthorized access to systems, applications, and data. Technologies and procedures that reduce the risk of unauthorized access to information systems shall be implemented.

Refer-ChrysCapital-ISMS-Password Management Procedure V1

5.2 Capacity Management:

ChrysCapital shall ensure that the use of key resources such as server, CPU, memory, network bandwidth, and UPS capacity is continuously monitored and evaluated to meet both current and future demands. Capacity planning shall ensure continuous availability of critical resources as per the business's operational requirements.

5.3 Protection against Malware:

It shall be ensured that appropriate preventive, detective, and corrective controls are implemented to protect information systems from malicious software. Employees of ChrysCapital shall not write, generate, compile, copy, collect, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage or otherwise hinder the performance of any ChrysCapital information assets. It shall be ensured that:

a) ChrysCapital approved antivirus protection software is installed on all workstations and are kept up to date.

b) Malicious websites are blocked using proxy or content filtering solution.

c) Incoming internet web traffic as well as attachments are scanned for malicious content.

5.4 Data Retention and Deletion:

It shall be ensured that the method of deletion is appropriate to the type of information, following secure and thorough procedures to ensure data is irrecoverable. When working with third parties, ChrysCapital shall ensure that the deletion of information is properly documented and conducted as per agreed contractual obligations.

Implementation

a) A deletion method shall be selected based on business requirements and the type of data being deleted.

b) Detailed records of data deletion activities, including the method used and the results of the deletion shall be maintained.

Refer-ChrysCapital-ISMS-Backup and Restoration Procedure V1
Refer-ChrysCapital-ISMS-Asset Management and Media Disposal

5.5 Data Masking:

Data masking shall be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies and business requirements. ChrysCapital shall ensure that data masking processes comply with legal, statutory, regulatory, and contractual requirements, particularly in contexts like healthcare or payment card processing. Implement privacy controls to ensure that personally identifiable information (PII) and other sensitive data remain protected from unauthorized viewing or access.

Implementation

a) Encryption and data obfuscation methods shall be implemented to ensure that unauthorized users cannot access sensitive data.

5.6 Data Leakage Prevention:

ChrysCapital shall implement data leakage prevention (DLP) measures to secure sensitive data in IT systems, networks, and devices, preventing unauthorized access or transfer. Utilize advanced DLP tools and technologies to prevent, detect, and block data leakage across endpoints, networks, and cloud services.

Implementation

a) DLP controls across all systems, networks, and devices, including email services, file transfers, and portable storage shall be activated.

b) DLP systems to detect specific types of sensitive information and quarantine emails or files that contain such information shall be configured.

5.7 Backup and Restoration:

Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy. Regular backups shall be taken for all essential business information; a backup plan shall be documented identifying the information systems, information to be backed up, type and frequency of backups. All back up activities shall be logged through an event trail. It shall be ensured that:

a) Information systems are backed up at frequency adequate to meet business requirements.

b) Backup data shall be stored securely and would be easily available.

c) Integrity of backup copies shall be tested at periodic interval.

Refer-ChrysCapital-ISMS-Backup and Restoration Procedure V1

5.8 Redundancy of Information Processing Facilities:

ChrysCapital shall implement redundancy in critical information processing systems. Ensure redundancy is designed to meet the availability and service obligations outlined in the organization's Business Impact Analysis (BIA) and continuity plans. Redundancy systems shall be regularly tested to confirm they are functioning as expected and can be activated when needed during a disruption.

Implementation

a) Ensure physically redundant power supplies to maintain operations in case of a power outage.

b) Test the redundancy systems regularly to ensure they function as required.

5.9 Logging and Monitoring:

Logs related to activities, exceptions, faults, and other relevant events across networks, applications, and IT systems shall be generated, stored, protected, and regularly analyzed.

Event logging shall be enabled for at least critical systems (e.g., crown jewel application servers, L3 Network devices, firewall, antivirus etc.) to capture details about all the important events and monitor it. Monitoring of all logs of events and incidents shall be done to identify unusual patterns and behaviors.

Refer-ChrysCapital-ISMS-Operations Management Process V1

5.10 Use of privileged utility programs:

ChrysCapital shall restrict the use of privileged utility programs (e.g., diagnostic tools, antivirus, backup software) to authorized personnel only, ensuring that only the minimum necessary individuals have access.

Implementation

a) Access to privileged utility programs shall be restricted to the minimum number of authorized users.

b) Robust identification and authentication procedures shall be used for accessing utility programs.

Refer- ChrysCapital-ISMS- Access Management process V1

5.11 Network Security:

ChrysCapital shall protect sensitive data from unauthorized access or interception during transmission across the network, ensure data consistency by preventing unauthorized modifications, tampering, or corruption, ensure continuous availability of network services and minimize downtime through proactive threat management and robust network design, detect, mitigate, and respond to potential network threats, including malware, intrusion attempts, and unauthorized access.

5.12 Change Management:

ChrysCapital shall ensure that all changes to information systems and processing facilities are documented, controlled, and reviewed through a formal change management procedure. Detailed records of all changes and updates shall be maintained.

Implementation

a) A formal change management procedure shall be established that defines how changes to systems and processes are requested, reviewed, approved, and implemented.

b) Ensure that every change is documented, including its scope, purpose, potential risks, and impact on other systems or processes.

Refer-ChrysCapital-ISMS-Change Management Process V1

5.13 Protection of Information Systems During Audit Testing:

ChrysCapital shall establish clear guidelines and processes to manage access requests during audit testing, ensuring that only necessary data and systems are accessed. Implement controls to limit the scope and potential impact of audit tests on operational systems, reducing risks to business continuity and data integrity. Ensure that any devices used for accessing information systems during audits (e.g., laptops, tablets) meet security requirements. Audit requirements on the operational systems shall be planned, documented, and agreed to minimize the risk of disruptions to business processes. Specific scope of technical audit shall be defined and agreed before starting, ensuring only necessary systems and data are accessed.

VI. Legal, Statutory, Regulatory and Contractual Requirements:

ChrysCapital shall identify, document, and comply with all applicable legal, statutory, regulatory, and contractual requirements relevant to information security.

Implementation

1. The organization shall begin by identifying all legal, statutory, regulatory, and contractual requirements that apply to its information security practices such as data protection laws, and contractual obligations related to clients or partners.
2. Once identified, these requirements shall be documented clearly. The documentation shall be regularly updated as new laws come into effect or existing laws are amended.
3. Roles and responsibilities of individuals within the organization shall be identified for ensuring compliance.

VII. Cyber Security:

7.1 Threat Intelligence:

ChrysCapital shall gather, analyze, and deliver actionable threat intelligence that is relevant, timely, and aligned with the organization's needs to enhance security posture and support proactive defense strategies.

Implementation

a) Credible data sources shall be selected from both internal and external environments.

b) Processed intelligence shall be communicated to stakeholders in an understandable format.

7.2 Third Party Risk Management:

ChrysCapital shall identify, manage, and mitigate the security risks associated with third-party suppliers, including the protection of sensitive data. This shall be achieved by establishing security requirements within supplier contracts.

Implementation

a) Suppliers' security practices shall be assessed to ensure they align with organizational requirements.

b) Secure data transfer or destruction shall be ensured during and after supplier contract termination.

Refer-ChrysCapital-ISMS-Third Party Risk Management Process V1

7.3 Business Continuity and Recovery:

ChrysCapital shall maintain a robust level of information security during disruptions, such as disasters or interruptions, by establishing Business Continuity Management System (BCMS) at adequate level to meet the continuity and recovery objectives of the business process and/or associated information systems.

Implementation

a) Response and recovery plans shall be developed and regularly tested to safeguard business processes during disruptions.

b) The response and recovery plan shall have plans for the timely restoration of systems affected by incidents of cybersecurity incidents/attacks or breaches (for instance, offering alternate services or systems to customers).

Refer-ChrysCapital-ISMS-Cyber Resilience Policy V1

7.4 Technical Vulnerability and Patch Management:

ChrysCapital shall continuously identify, monitor, and assess vulnerabilities in information systems, including endpoints, servers, network devices, cloud environments, applications and take prompt and appropriate actions.

Implementation

a) A timeline and process for responding to notifications of relevant technical vulnerabilities shall be defined.

b) It shall be ensured that updates, patches, and fixes are obtained from legitimate sources.

Refer-ChrysCapital-ISMS-Operations Management Process V1

7.5 Incident Management:

ChrysCapital shall effectively manage, assess, and respond to information security incidents by establishing clear processes for incident detection, response, containment, and recovery.

Implementation

A comprehensive incident management plan outlining procedures for various incident types shall be established. The plan shall be regularly tested and updated to evolving threats.

a) Systems for detecting and reporting incidents shall be implemented with defined escalation criteria.

b) A process for classifying incidents based on severity and impact shall be established.

Refer-ChrysCapital-ISMS-Cyber Resilience V1

VIII. Non-Compliance:

All employees, contractors, third-party vendors, and any other individuals or entities that access or handle the organization's information systems, networks, and data) shall be required to comply with the ChrysCapital-Information Security Policy as applicable. Non-compliance with the ChrysCapital-Information Security Policy shall be dealt in accordance with the disciplinary process of ChrysCapital.

ChrysCapital Advisors LLP

502 Ceejay House, Dr. Annie Besant Road,
Worli, Mumbai 400 018. INDIA.

+91 22 4066 8000

www.chryscapital.com