1.0 PURPOSE AND INTRODUCTION

The use of Information Technology ("IT") is critical to the success of Coherent Corporation ("Coherent", the "Company"). However, these technologies introduce risks and the cybersecurity threat landscape changes continuously. Mitigating threats to Coherent information and information assets requires contributions from all employees for security controls to be effective.

The objective of this Coherent Security Policy for Information Technology and Networks (the "Policy") is:

- To help prevent or minimize the impact of information security incidents, to protect Coherent business interests, and to safeguard our people;
- To present the approach Coherent takes for protecting its information and information assets; and
- To define the responsibilities of all parties in protecting Coherent information and information assets.

This Policy enables Coherent to meet its legal obligations and to take appropriate measures to minimize potential risks to Coherent and its operations. This Policy is also meant to fulfill contractual and regulatory obligations. It will help ensure Coherent is able to fulfill the needs and expectations of its business partners and constituencies – customers, suppliers, employees, shareholders and the community.

2.0 SCOPE

This Policy applies to all employees, contractors, consultants, temporary personnel, personnel affiliated with external parties, and anyone who uses computer-based information assets and networks that support Coherent business operations globally ("Users").

Among the parties that utilize Coherent information assets are:

1. Employees requiring access to perform activities associated with his/her work assignment.
2. Temporary or contract personnel who require system access to fulfill the requirements of his/her assignment.
3. External parties such as:
    a. Business Partners (e.g. customers, suppliers) with whom we interact electronically.
    b. Supplier personnel who require system access to provide hardware and software maintenance services on a computer system, network, or to the physical plant.

All Users are required to abide by this Policy and the security standards outlined in this Policy.

The Information Assets in scope of this Policy include all digital systems that store, process or transmit data owned or controlled by Coherent. The scope of this Policy includes single-user and shared computers and servers and their associated applications; Industrial Control Systems ("ICS"); mobile and handheld devices; Coherent-owned services hosted on the internet or in public or private clouds; and network communication facilities that support the delivery of information and applications to the Coherent user base, including third-party carrier services.

This Coherent Security Policy for Information Technology and Networks applies to all fully or majority owned subsidiaries. Coherent subsidiaries, business units, divisions, or teams may establish

information security policies or standards that are specific to their subsidiary, business unit, division, or team, however, such policies or standards must reference this Policy. Where those policies conflict with this Policy, this Policy takes precedence.

3.0 RESPONSIBILITY

Ownership of and the authority to conduct information security activities is vested in the Coherent Chief Information Officer ("CIO"). The CIO provides strategic guidance to the senior Coherent Cybersecurity Official and reports status of organizational objectives to executive stakeholders. The CIO approves and provides oversight of the Coherent Cybersecurity Program.

It is the responsibility of the senior Coherent Cybersecurity official to maintain, communicate, review, and continuously improve this Policy and the measures and activities described herein (collectively the "Coherent Cybersecurity Program" or the "Program"). The senior Coherent Cybersecurity official will review and update this Policy and the Program at a minimum of once per year and when significant changes are made to the Coherent computing environment, or as required by applicable regulation or law.

The senior Coherent Cybersecurity official is responsible for defining and documenting the minimum set of requirements for the Coherent Cybersecurity Program ("Security Standards" or "Standards").

In consultation with the senior Coherent Cybersecurity official, the Coherent Vice President of Corporate and Global IT operations is responsible for developing and maintaining documented instructions for routine IT activities that adhere to this Policy and the Standards it prescribes ("IT Procedures", "Procedures").

The senior Coherent Cybersecurity official is responsible for implementing the Coherent Cybersecurity Program as outlined in this Policy. The Program shall include trained personnel with formally assigned responsibilities, Security Standards and Procedures, and digital and physical tools to address, at a minimum, the cybersecurity domains outlined in this Policy.

All Users, including non-IT personnel, who own or administer Information Assets, including Industrial Control Systems, on behalf of Coherent, shall be familiar with and implement this Policy and the Security Standards and Procedures.

All Users are responsible for reporting violations and suspected violations of this Security Policy or its Standards to the responsible system administrator, Internal Audit department, the senior Information Security official, or IT management. Serious violations may be reported to Senior Management through appropriate channels.

Any exceptions to this Policy or the Standards must be approved in writing by the senior Coherent Cybersecurity official.

4.0 KEY TERMS

Baseline Configurations are a documented set of specifications for information systems that has been formally reviewed by the Coherent Information Security Program and which can be changed only through Coherent change control Procedures.

The term "**Coherent Corporation**" or "**Coherent**" encompasses the Coherent Corporation organization and its divisions and subsidiaries, either wholly or majority owned.

The **Coherent Enterprise Network** (or **"CEN"**) is the collective information processing capability controlled by Coherent that stores, processes, and transmits sensitive Company information, including all IT Assets hosed in Coherent sites and any device that is controlled by Coherent, whether that information is cloud-based, on-premises, mobile, or processed elsewhere.

Industrial Control Systems or **"ICS"** is broadly defined term that encompasses any type of supervisory, historian, or control systems and associated instrumentation used in industrial or manufacturing processes.

Information Assets refers to all Coherent computer-based data, the applications used to maintain the data, backup copies of the information, output from the computer-based information systems and the resources which facilitate the delivery of this information to its users, for example, hardware, software and communications networks. Also known as **Computer-Based Information Assets** or **Assets**.

Information security is sometimes referred to as **cybersecurity** and refers to the confidentiality, integrity and availability of data and IT assets.

Information technology is the study or use of systems (especially computers and telecommunications) for storing, retrieving, and sending information.

Least Privilege Principle states users, devices, and processes must be able to access only the information and resources necessary for their legitimately assigned duties. Also known as the principle of minimal privileges or the principle of least authority.

Need-to-Know is a term that described access limitations that, even if a user, device, or process has approval to access certain information or information systems, access will be granted only if the subject has a specific need to know. Access to Coherent information must be necessary to perform officially assigned duties.

A Coherent **Standard** is a Coherent policy document with more technical detail than a Policy. Both Policies and Standards direct Coherent personnel action, but Standards only apply to a limited set of users (such as IT Administrators). Policies generally apply to all or most users.

Users are employees, contractors, consultants, temporary personnel, personnel affiliated with external parties, and anyone who uses Computer-Based Information Assets and networks that support Coherent business operations globally.

5.0 THE POLICY

Coherent will identify information security requirements through a risk assessment process and implement measures necessary to meet those requirements. Coherent information and Information Assets shall be safeguarded from unauthorized access, disclosure, modification, destruction, and use. Security responsibilities will be communicated to all Users.

The Coherent Information Security Program will implement this Policy through formal duties and job descriptions assigned to qualified personnel, documented standards and procedures, and applications and tools dedicated to, at a minimum, the following domains.

> Access Control – A portfolio of technologies and policies to ensure access to Coherent information and information systems is limited to authorized users and devices. Access will be controlled based on the principles of Least Privilege and Need-to-Know. Accounts with elevated privileges shall be controlled.

Awareness, Training and Education – All Coherent personnel will have the knowledge necessary to securely operate IT Assets and they will understand the Company's expectations for how IT Assets should be used. Users with cybersecurity responsibilities will have the expertise necessary to perform their duties.

Audit and Accountability – Computer logs will be created and retained to facilitate the monitoring, analysis, investigating, and reporting of system activities. The logs will be reviewed for unauthorized activity.

Configuration Management – The collection of people, processes, and tools to maintain an inventory of information and Information Assets. Baseline Configurations and consistent minimum-security standards shall be established and enforced to ensure only authorized users and processes are able to access or execute authorized services.

Identification and Authorization – This subprogram is dedicated to limiting access to only authenticated entities for legitimate and approved business purposes. Its Standards will detail security requirements for individuals and devices that access Information Assets so it can be shown they are indeed who they represent themselves to be. Authentication mechanisms shall be commensurate with the value of the information they are protecting.

Incident Response – Capabilities to prepare for, detect, analyze, contain, respond to, and recover from adverse security events. Security events will be tracked and documented and reported to relevant parties, such as customers, partners, and senior Coherent leadership, as required by law, regulation, or contract, and when necessary or desirable.

Maintenance Security – Preserve and protect Coherent information systems by making sure they are in good working order and information is protected during repair and upgrade activities.

Media Protection – The tools and processes needed to secure digital media during its active lifecycle and sanitized or destroyed before it is disposed of or reused.

Personnel Security – Measures to protect Information Assets from people, including the vetting of individuals prior to being given access to Coherent information systems. Standards shall be established to ensure Coherent information and Information Assets are protected during and after personnel actions such as termination or transfers.

Physical Protection – Limitations on and monitoring of physical access to Coherent digital equipment and the environment it operates in.

Risk Assessment – Procedures and tools for security personnel to inform Coherent leaders and managers of the levels of risk associated with the operation and use of Information Assets. The Coherent Cybersecurity team shall establish a methodology for assessing the enterprise-level information security risk on a periodic and ongoing basis. All Information Assets will be assessed for risk and risks will be mitigated, avoided, or accepted by a Vice-President-level manager before given the authority to operate.

Security Assessment – The Information Security team will develop the tools and procedures to assess CEN security controls on a continuous basis, at least once per year, and when significant changes are introduced. Business-unit-, department-, and system-level assessments will be performed when needed. The capability to develop plans to correct deficiencies found in assessments will be established.

Situational Awareness – Establishes tools and processes to gather and disseminate cyber intelligence effectively so Coherent personnel understand how to make good decisions about keeping Coherent interests, its assets, and its employees safe and secure.

System and Communication Protection – The Coherent Enterprise Network will be governed by architectural designs, software development techniques, and systems engineering principles that promote effective information security. Coherent communications will be monitored, controlled, and protected.

System and Information Integrity – The capability to monitor for, analyze, and remediate software flaws including the tools and processes needed to protect against malicious software code.

Information Assets, including ICS devices, that do not adhere to the standards prescribed here are not allowed to be operated by Coherent personnel, or connected to the CEN, without the express written approval of the senior Coherent Information Security official.

6.0 WHAT ARE THE CONSEQUENCES FOR FAILURE TO COMPLY WITH THIS POLICY?

It is acknowledged that, in rare circumstances, certain Users will need to employ systems that are not compliant with the Coherent Standards. All exceptions require advanced, written approval from the senior Coherent Information Security official.

Any employee found to have violated this Policy or the Standards mandated by this Policy will be subject to disciplinary action; this action may include one or more of the following:

- Issuance of verbal or written warning.
- Documentation of violation in employee's personnel file.
- Termination of employment.
- Initiation of legal action to enjoin violations and/or collect damages, if any, caused by violations.
- Criminal prosecution is possible, depending on the situation.

Any consultant, contractor or temporary worker found to have violated this Policy will be subject to the same disciplinary action as an employee as applicable to their status. Cancellation of any agreement between Coherent and the party may also occur.

7.0 QUESTIONS AND REPORTS

If you have a question about this Policy, contact your local IT representative, Cybersecurity@Coherent.com, the senior Coherent Cybersecurity official, or the Coherent Chief Information Officer.

8.0 COMMUNICATION

This Policy and any future changes will be communicated by the approvers. The Company reserves the right to modify this Policy, as needed, to reflect changes in applicable laws or otherwise.

APPROVALS (through Electronic Workflow)	COMPLETED DATE
Vice President of Global and Corporate IT Operations Dale Bynum	1/18/2023
Chief Information Officer Anantha Ganga	1/18/2023

APPROVALS (through Electronic Workflow)	COMPLETED DATE
President Bob Bashaw	2/14/2023

REVISION HISTORY

Revision	Date	Description of Change	Requested By
1.0	April 1, 2005	Policy created	
3.0	October 20, 2018	Updated with additional controls	K. Varley
4.0	November 1, 2020	Policy harmonization with Finisar Policies	D. Bynum
5.0	October 3, 2022	Updated Company name from II-VI Incorporated to Coherent Corp. Changed branding and formatting to adhere to the new Coherent policy guidelines. Added Table of Changes. Added the creation of procedural documentation to IT Management responsibilities Updated throughout to define the Information Security Program and its specific security domains. Removed granular and low-level requirements for system settings and procedural staff directives. These details are moved to their respective sub-policy, process document, or procedure.	D. Bynum