The Israeli Cyber Emergency Response Team (CERT) Principles of Operation

Cybersecurity Best Practices

B.19

Volume B:
A technical approach

IDB

INCD
Israel National
Cyber Directorate

This document was originally published by the Israel National Cyber Directorate (INCD) in Hebrew. Its translation into English was carried out by the cybersecurity team of the Innovation in Citizen Services (IFD/ICS) division of the Inter-American Development Bank (IDB), and it is included as a chapter of the "Cybersecurity Best Practices" collection.

The reader should keep in mind that cybersecurity is a rapidly evolving field. Although these documents reflect established principles, they may be periodically updated as necessary to reflect developments in this field. Additionally, while every effort has been made to present the recommendations and resources in a way that is universally applicable to organizations around the world, the reader may find references that are specific to Israel's cyberecosystem and context (such as the amounts indicated in New Israeli Shekels [NIS], or references to Israeli law or government agencies).

The original document is available at: **https://www.gov.il/he/pages/principles**. Please note that it includes the following disclaimer:

Contents

Foreword

Digital Transformation and the Challenges of Cybersecurity

As digital transformation continues to expand throughout the world, governments, organizations, individuals, and even objects are increasingly connected to the internet. Although digitalization offers undeniable benefits, such as efficient public service delivery, economic growth, and essential connectivity, it also contributes to our growing collective exposure to cybersecurity risks. Recently, the global COVID-19 pandemic has been an important driver of this phenomenon. As a result of widespread social distancing policies, the number of e-commerce transactions and online personal communications grew sharply in a short period of time, along with the number of employees who began teleworking for the first time. In this unprecedented situation, many internet users undertook novel online interactions without enough awareness of the security risks involved. Organizations had to quickly adapt to these challenges by setting up fully remote workflows, often without all of the necessary security measures in place or appropriate guidance to employees.

Cybercriminals are quick to exploit the uncertainty and vulnerability of unsuspecting individuals. Phishing and other social engineering scams proliferated, taking advantage of the global need for information related to the pandemic and the massive use of videoconference applications. In April 2020, Google reported more than 18 million daily malware and phishing emails related to COVID-19 in only a week. Hackers posing as the World Health Organization sent phishing emails and massively spread malicious links to fake videoconference meetings and attachments containing malware. According to the Check Point Research 2021 Security Report, in the first few months of 2020, almost a million attack attempts against Remote Desktop Protocol (RDP) connections, widely used among organizations for employees' remote connections, were observed every day. In fact, RDP attacks were the most popular form of cyberattack, surpassing even phishing emails. In the second half of the year, as more organizations strengthened the security of their remote platforms, hackers focused their efforts on exploiting vulnerabilities in employees' private assets and remote access devices to penetrate their organizations. Although such threats were maximized by this global context, they are not novel and will not go away; we continue to live in an environment of heightened risk, which is particularly serious in regions of the world where cybersecurity policies and technology are less developed and where citizen education and awareness around this issue are lacking. In other words, although the shifts due to the COVID-19 pandemic may revert to what they were before the pandemic, they have brought to light the urgent need to strengthen individual and collective protections against cyberrisks.

Strengthening cybersecurity is essential to safeguard citizens' rights to privacy and property in the digital sphere, promote citizens' trust in digital technologies, and support economic growth through safe digital transformation. In particular, citizens must be assured that the digital systems they use for their personal or professional activities, as well as those that involve their personal data, possess adequate security measures to guarantee the integrity, confidentiality, and availability of their information and the services that they need. Moreover, security breaches have a significant negative economic impact. A recent report by McAfee estimated that cybercrime costs the world economy around US$6 trillion annually, or 0.8 percent of global GDP.

Israel: A Global Leader in Cybersecurity

Israel's innovation and entrepreneurship ecosystem is globally recognized as one of the most vibrant in the world, earning it the name Startup Nation. According to the March 2021 OECD Science and Technology Indicators, Israel is the country that invests the highest percentage of its GDP (4.9 percent) in research and development (R&D). The country is host to more than 300 research and development and innovation (R&D&I) centers of multinational companies. Of these, dozens are dedicated to cybersecurity.

It is no surprise that 40 percent of all private investment in cybersecurity worldwide takes place in Israel, which also has one of the world's largest private ecosystems in this area, second only to that of the United States. According to 2021 data, in that year US$8.8 billion were invested in around 131 Israeli companies from this sector, and more than 40 were acquired for a total of US$3.5 billion. Israel has more than 500 cybersecurity startups, and by 2021, 33 percent of the world's "unicorns" were Israeli. Overall, Israel's export of cybersecurity products was estimated in 2020 at US$6.85 billion.

The Israel National Cyber Directorate (INCD) is responsible for securing Israel's national cyberspace and for establishing and advancing its cyberresilience. The INCD operates at the national level to constantly raise the level of security of organizations and citizens, to prevent and manage cyberattacks, and to strengthen cyberemergency response capabilities. Its positioning as part of the Prime Minister's Office clearly demonstrates the centrality and importance of its responsibilities. Its goals include to prepare and enable the Israeli private sector and general public to protect themselves from cyberthreats by adopting cybersecure technologies, publishing best practices, training personnel, and raising awareness. Furthermore, it aims to establish and strengthen the cyberscience and -technology base by developing highly qualified human capital, supporting advanced academic research, engaging in deep technological R&D, and fostering the cyberindustry. The INCD strives to maintain a protected, safe, and open cyberspace for all of the State of Israel's population and businesses and to facilitate the country's growth and its scientific and industrial base.

The State of Cybersecurity in the Latin American and Caribbean Region

The Inter-American Development Bank (IDB) carries out periodic assessments to capture the evolving capacities of its member states to defend themselves against the growing threats in cyberspace. The 2020 Cybersecurity Report, "Risks, Progress, and the Way Forward in Latin America and the Caribbean," developed in partnership with the Organization of American States (OAS), showed that countries were at varying stages of development in their preparedness to face cybersecurity challenges, but generally still had ample room for improvement.

While in 2016, the year of the report's first edition, 80 percent of the countries in the region did not have a national cybersecurity strategy in place, this number had only fallen to 60 percent by 2020. Furthermore, only a few countries manage the exposure of their critical infrastructure, such as their energy, healthcare, telecommunications, transportation, water supply, and financial sectors, to cyberattacks. As revealed by the 2020 report, only 7 countries of the 32 assessed had a critical infrastructure protection plan in place. This is one of the most worrisome findings of all, considering the catastrophic impact that attacks on these sectors could have not only on national economies, but on the lives of all their citizens.

In terms of countries' capacity to manage and respond to cybersecurity incidents, the same study found that 63 percent of countries had security incident response teams in place, such as computer emergency response teams (CERTs) or cybersecurity incident response teams (CSIRTs). However, of the 20 countries that did, only 3 had reached advanced maturity in their ability to coordinate such responses. In fact, 23 out of the 32 countries were still in an initial stage of maturity in this respect. This finding underscored the general need for countries to strengthen the capacity of their teams to effectively coordinate their responses to cyberincidents. Moreover, the report examined the availability of educational and training opportunities in cybersecurity and found that fewer than half of the countries in the region offered formal education in cybersecurity, such as postgraduate, master's, or technical degrees. Needless to say, having sufficient trained professionals is essential to design and implement the cybersecurity policies and measures that are necessary to ensure a country's resilience in the face of increasingly sophisticated and complex cyberattacks.

The Inter-American Development Bank's Support to Strengthen Cybersecurity Capacity in the Region

For the past few years, the IDB has actively supported the region in the development of cybersecurity capacity, the design and implementation of national-level cybersecurity policies, and the strengthening of cybersecurity capabilities in the sectors it helps develop. This support takes a number of forms. The IDB has provided financial assistance amounting to tens of millions of dollars to develop national cybersecurity capabilities through more than 15 public sector investment loan operations, as well as significant additional funding to ensure the cybersecurity of digital transformation investment projects.

It also provides technical guidance and conducts cybersecurity projects across the region through consultancies, assessments, and tailor-made cybersecurity-strengthening projects on topics that include critical infrastructure protection, cybercrime and forensic analysis, design and strengthening of CSIRTs and security operations centers (SOCs), and national and sectoral cybersecurity strategies. In addition, the IDB has made substantial efforts to provide opportunities for Latin American and Caribbean professionals to strengthen and update their skills in this field by regularly offering workshops and training opportunities. These have included two-week cybersecurity executive courses, offered jointly with the Hebrew University of Jerusalem, as well as tailor-made courses on critical infrastructure protection and others targeted for specific sectors. Finally, the IDB has produced several high-impact publications dealing with national and sectoral cybersecurity issues, and continues to update and add to this body of knowledge regularly.[1]

1. See the website of the Data and Digital Government Cluster (DDG) of the IDB's Innovation in Citizen Services (ICS) division: **https://www.iadb.org/en/who-we-are/topics/modernization-state/data-and-digital-government**.

The IDB and the INCD: Joining Forces

The challenges of cybersecurity, like those of the internet itself, are global. Thus, sharing the knowledge and tools to meet these challenges benefits everyone. In recognition of this reality, the INCD and the IDB have partnered to make Israel's expertise in this area accessible to LAC countries. This collaboration has supported the LAC region in the form of executive and technical trainings on advanced cybersecurity topics, cutting-edge conferences for LAC public officials and professionals in the field, and innovative technical assistance projects. This publication is a product of this collaboration. It consists of a series of cybersecurity methodological guides for organizations, developed by the INCD in light of its analysis of risks, attack methods, cyberincidents, and globally accepted standards. These guides have been translated into Spanish and English as a joint activity of both organizations. They are being made available in these languages with the aim of providing access to this body of knowledge to audiences throughout the LAC region and contributing to strengthening cyberresilience in the region.

The challenge of protecting the digital space will continue to grow, along with the need for proven expertise to confront it. The insights contained in these guides are a resource to promote much-needed professional training in cybersecurity in the LAC region. These guides will contribute to raise organizational standards, promote greater awareness and a culture of cybersecurity within organizations and among the general public, and inform decision makers, managers, and leaders in their cybersecurity initiatives. It is our hope that these guidelines will serve as a roadmap for professionals and leaders throughout the LAC region, working together to build a more secure and prosperous future.

/01. Definitions

01

Cyberincident: A breach or an actual threat of a breach of the cyberdefense policy in a computerized system or a violation of the use of a computerized system as planned or of its security, including:

- Disrupting the proper operation of a computer or interfering with its use.
- Deleting computer material, modifying it, disrupting it in any way, or interfering with its use.
- Storing false data on a computer or displaying false output (data or output that is misleading, depending on the purposes for which it is used).
- Illegally penetrating into computer material.
- Eavesdropping on communication between computers.
- Exposing data stored on a computer to a person unauthorized to view it.

02

Entities with whom there are collaborations: Entities involved in the field of cyberdefense with which the Cyber Emergency Response Team (CERT) cooperates within its mission, including parallel bodies around the world, the security community, the Israeli Police, the Privacy Protection Authority in the Ministry of Justice, international forums, and global companies in communications, computing, and cyberdefense.

03

Cyberdefense: A set of actions to prevent, neutralize, investigate, and address cyberthreats and cyberincidents, and to reduce their impact and the damage caused by them, before, during, and after they occur.

04

The CERT: Crisis center for dealing with cyberthreats established within the Israel National Cyber Directorate (INCD).

05

The INCD: The Israel National Cyber Directorate created in accordance with Government Resolution 2444 on the subject of "Promoting National Preparedness for Cyber Defense" of February 15, 2015.

06

Information of security value (actionable information): Any of the following:

- **Indicators:** Information from which it can be deduced that a cyberincident may have occurred, may occur, or is occurring (including peripheral information concerning the detection, identification, and investigation of threats and events with an emphasis on raw technological information).
- **Vulnerabilities:** Vulnerabilities in computer systems, their components, or related procedures that can be exploited to create a cyberincident.
- **Threat:** A threat of a cyberincident.
- **Malicious artifacts and software (malware):** Capabilities and tools used to exploit vulnerabilities.
- **Methodologies and tools:** Methodologies, capabilities, and tools for identifying cyberthreats and addressing and containing cyberincidents.

07

Unidentified information: Information, including protected information, that cannot be reasonably identified by the individual or organization it describes.

08

Protected information: Any of the following:

- Information to which the [Israeli] Protection of Privacy Law of 1981 applies to a single matter.
- Information on an organization that is not public.
- Commercial secrets under the [Israeli] Commercial Torts Law.

09

The CERT's systems: The hardware and software systems used to perform CERT tasks.

10

Target audience (constituencies): Actors in the economy that the CERT assists in its mission, including organizations and companies from all sectors; government ministries; communications and internet vendors; companies for cyberdefense products, consulting, and services; cyberdefense professionals; and the general public.

/02. Mission

01

The CERT is established within the INCD and as part of its mission.

02

The CERT's mission is to assist the entire economy in dealing with cyberthreats, including:

- Improve cyberdefensive resilience.
- Assist in dealing with cyberthreats.
- Assist in dealing with cyberincidents.
- Assemble and share valuable information with all actors in the economy.
- Serve as a central interface point between the security entities and the economic actors for the purposes of cyberdefense.

03

The CERT will not perform actions unrelated to this mission.

04

The CERT will balance the needs of cyberdefense with the protection of basic rights when exercising its mission.

05

The list of the CERT's services appears in Appendix 1 and is updated periodically on the INCD's website: **https://www.gov.il/en/departments/israel_national_cyber_directorate/govil-landing-page**.

/03.
Responsibility and Proper Management: Accountability

01

Overall responsibility for compliance with the CERT's principles of operation within the INCD's activities lies with the head of the INCD and includes the following tasks:

- Appointing the CERT's director from among the INCD's employees.
- Supervising the drafting of detailed work procedures for the CERT in accordance with these principles and examining the need to update them at least once a year in accordance with the CERT's activities.
- Establishing supervisory mechanisms for compliance with the principles.

02

The principles of operation outlined in this document will be implemented by the CERT using the methods and tools listed below, as appropriate:

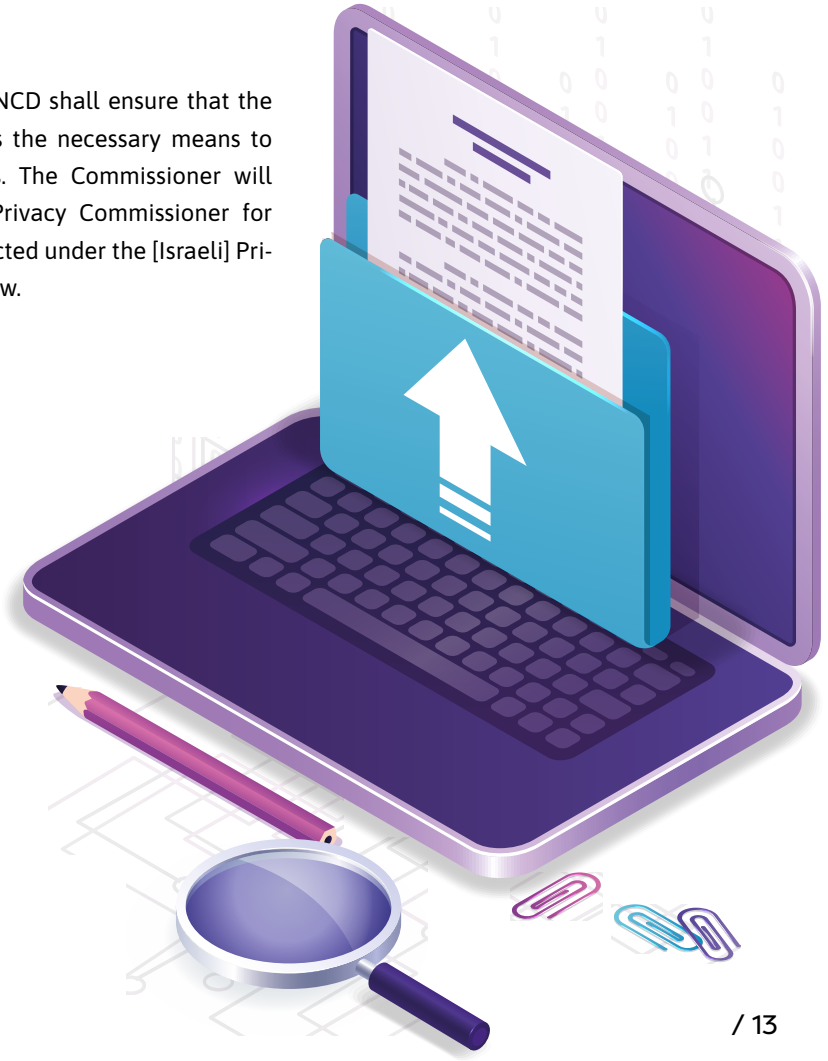
- Technological design of CERT systems.
- Technological controls in the CERT systems and supportive work processes.
- Regulation of work procedures.

03

The head of the INCD will appoint an employee (hereinafter "the Commissioner") from among the employees of the INCD who has been adequately trained to supervise compliance with these principles regarding protected information and monitor their implementation.

04

The head of the INCD shall ensure that the Commissioner has the necessary means to fulfill their duties. The Commissioner will also act as the Privacy Commissioner for information protected under the [Israeli] Privacy Protection Law.



/04. Receiving and Collecting Information

The CERT will collect information of security value for the needs of the CERT's mission and will do so from the sources mentioned below.

01

From an actor of the target audience after the following has taken place:

- The main points of these principles were presented to the actor.
- The actor was presented with a description of the traffic light protocol (TLP) distributed to the target audience or another protocol as determined in Chapter 7 (point 2) on classifying information, as specified in Appendix 2.
- The actor agreed to provide the information in accordance with these principles.
- If the contract contains protected information as defined by the [Israeli] Privacy Protection Law of 1981 for a single matter, the actor issued a notice to their employees and customers about cooperation with the CERT, which includes transferring information of security value from the organization to the CERT according to the wording of a message distributed by the CERT.

02

From actors with whom it cooperates.

03

From actors who are required to provide the CERT with information.

04

From any other legal source.

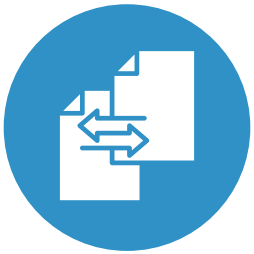
Collecting information containing protected information will be required to the minimum extent for the purposes of the CERT's mission. In the event that it becomes clear to the CERT that information has been collected that falls under the [Israeli] Privacy Protection Law of 1981 for a single matter, no use will be made of it and the information will be deleted, unless one of the following occurs:

01

The CERT has clarified that the information is collected and used with the consent of the individual to whom the information pertains in accordance with the [Israeli] Privacy Protection Law of 1981 and in accordance with the sensitivity of the information and how it is used.

02

The CERT's legal counsel has confirmed that the use of the information is urgently required to address a cyberincident, and that in the circumstances and given the sensitivity of the information and the severity of the incident, the information will not be used in violation of the [Israeli] Privacy Protection Law. If the legal counsel's approval is given under this section, the CERT will report this to the Attorney General.



/05.
Retention of Information in the CERT's Systems

01
The CERT has implemented information labeling rules that will allow it to indicate the sensitivity of the information, its level of sharing, and permissions in relation to its use.

02
Information will be retained to the extent possible in a way that will make it unidentifiable.

03
The CERT will use methods and measures to extract information of security value from protected information upon its receipt in a manner that reduces the need to preserve the raw protected information.

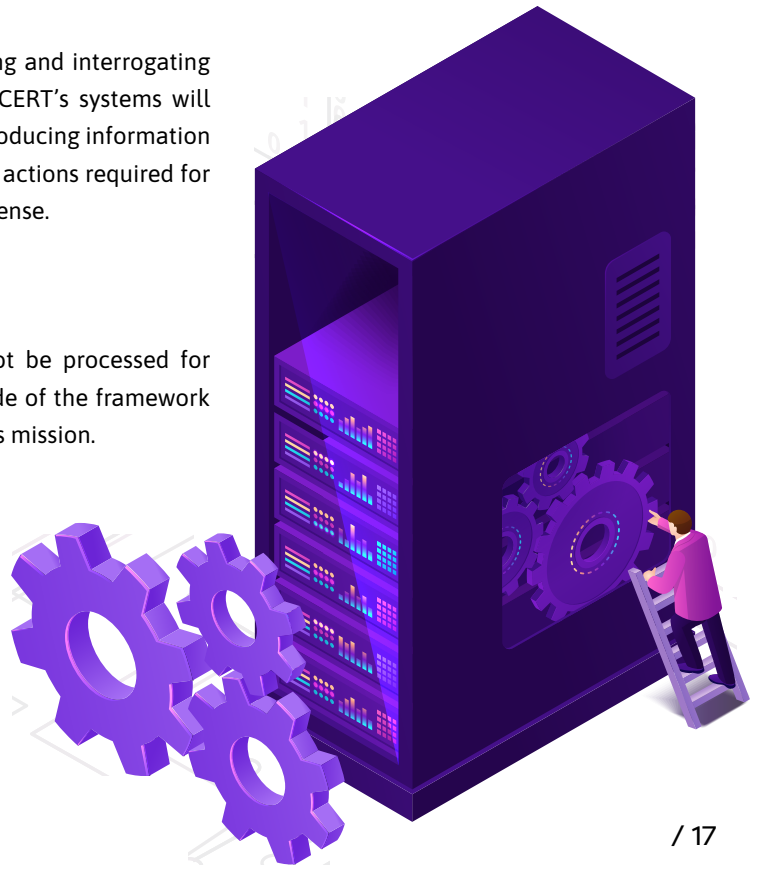
04
Raw information that has a reasonable possibility of containing protected information will be kept separately, and access to it will be limited to processes and designated employees in the INCD.

05
Protected information will be kept for the minimum period of time reasonably required for its use.

/06.
Information Processing

01
The activity of processing and interrogating the information in the CERT's systems will focus on locating and producing information of security value and on actions required for the purpose of cyberdefense.

02
The information will not be processed for purposes that fall outside of the framework of the CERT's and INCD's mission.



/07.
Distributing Information to the Target Audience

01
The CERT will distribute information of security value to the target audience only.

02
The CERT will distribute information to the target audience in accordance with the TLP or other protocol as published publicly by the CERT. Accordingly, the CERT will distribute information about the entity that reported to the target audience in an unidentified manner, unless the reporting entity has agreed to be identified.

03
The CERT will take reasonable measures to test the reliability of the information distributed.

04
The CERT will not be responsible for the use of the information distributed in the systems of the receiving organization.

05
The CERT will distribute information of security value that includes protected information under the [Israeli] Privacy Protection Law, only subject to the conditions of Chapter 4 of this document.

/08.
Cyberdefense and Information Security in the CERT's Operation

01
The CERT will make use of technology, procedures, and methods aimed at protecting its systems and information against tampering, alteration, or unauthorized access, taking into account the relevant risks.

02
These principles also apply to backup systems and the information stored in them.

/09.
Personnel: Access Permissions and Compartmentalization

01
The CERT's Director will determine role-based access permissions to the CERT's systems. Access will be granted for each role only to the extent required to perform their job.

02
The information will be accessed, to the extent possible, in a way that keeps the information unidentified, taking into account the CERT's mission.

03
The CERT's systems will have an automated documentation mechanism that will allow access to information in the CERT's systems to be controlled and monitored.

04
Permissions to the CERT's systems will be allocated according to the instructions of the CERT's Director after consulting with the Commissioner and after taking acceptable measures to test their suitability for access and use of the systems.

05
The Commissioner of protected information will conduct training for employees on duties in accordance with these principles and on laws applicable to protected information.

/10.
Controls

01
The CERT will implement, to the extent possible, automated mechanisms in its systems that will enable compliance with the principles and procedures to be monitored.

02
The Commissioner will oversee the control mechanisms for the purpose of detecting incidents of suspected misuse.

/11. Transparency in the CERT's Information Processing Activities

01

These principles will be made available for public inspection on the INCD's website.

02

The CERT will disseminate to actors with whom it cooperates recommendations regarding how to inform their employees and customers about cooperation with the CERT.

Appendices

Appendix 1. The CERT's Services

The list of the CERT's services is updated periodically on the INCD's website: **https://www.gov.il/en/departments/israel_national_cyber_directorate/govil-landing-page**.

Services

The CERT is designed to offer a variety of services that will be provided according to the characteristics of the threat, the incident, and the actors in the target audiences and subject to the rules of its operation. The types of services are defined according to the methodology developed by the world's leading bodies:

01

Reactive services: Offered in light of an incident, indication, report, or individual request, including alerts and warnings, assistance in handling incidents, and technological research to identify and analyze harmful files.

02

Proactive services: Provide assistance and information to improve the level of readiness and protection against future events, including information, training and practice, and proactive tests to detect threats.

03

Complementary security management services.

Appendix 2. Traffic Light Protocol (TLP)

TLP is an accepted method for classifying sensitive information that is not classified in the organization's information classification processes. Its purpose is to facilitate the sharing of information while defining restrictions and conditions regarding its distribution. This method creates a convention between the partners about the proper use of the information in order to enable the transfer of important protected information to all relevant parties while minimizing the fear of harm to the sharing party.

Table A2.1. Traffic Light Protocol

Sharing Restrictions of the Receiving Party	Classification	Purpose of the Classification
Information classified as **"red"** should not be shared with anyone outside the original group of recipients.	🔴	Cases where the information is of effective security value to other parties and may lead to a violation of the privacy, reputation, or activity of the sharing party if it is misused.
Information classified as **"yellow"** can only be shared with actors within the same organization, and only to the extent necessary in order to provide an effective response.	🟡	Cases where the effective use of information requires the participation of other parties, but expanding distribution beyond that may infringe on the privacy, reputation, or activity of the sharing party.
Information classified as **"green"** can be shared with all parties that may make productive use of it. However, do not share via public channels such as websites, social networks, and mass media.	🟢	Cases where the information may benefit many parties and its sharing does not involve a risk to the sharing party.
Information classified as **"white"** can be shared with any recipient group, including public channels.	⚪	Cases where there appears to be minimal or no risk at all in the distribution of information, subject to copyright.

The Israel National Cyber Directorate (INCD) is responsible for securing Israel's national cyberspace and for establishing and advancing its cyberresilience, operating to constantly raise the level of security of organizations and citizens, to prevent and manage cyberattacks, and to strengthen cyberemergency response capabilities.

In this context, the Israeli Cyber Emergency Response Team (CERT) was established within the INCD and as part of its mission. Its aim is to provide assistance in dealing with cyberthreats to the entire economy—organizations and companies from all sectors; government ministries; communications and internet vendors; companies offering cyberdefense products, consulting, and services; cyberdefense professionals; and the general public—by assembling and sharing valuable security information with all these actors.

This document describes the Israeli CERT's principles of operation, purpose, management principles, and policies for the processing and sharing of information, in order to establish the transparency of its activities and ensure that there is a balance between the nation's cyberdefense needs and the protection of basic rights of the public when exercising its mission.

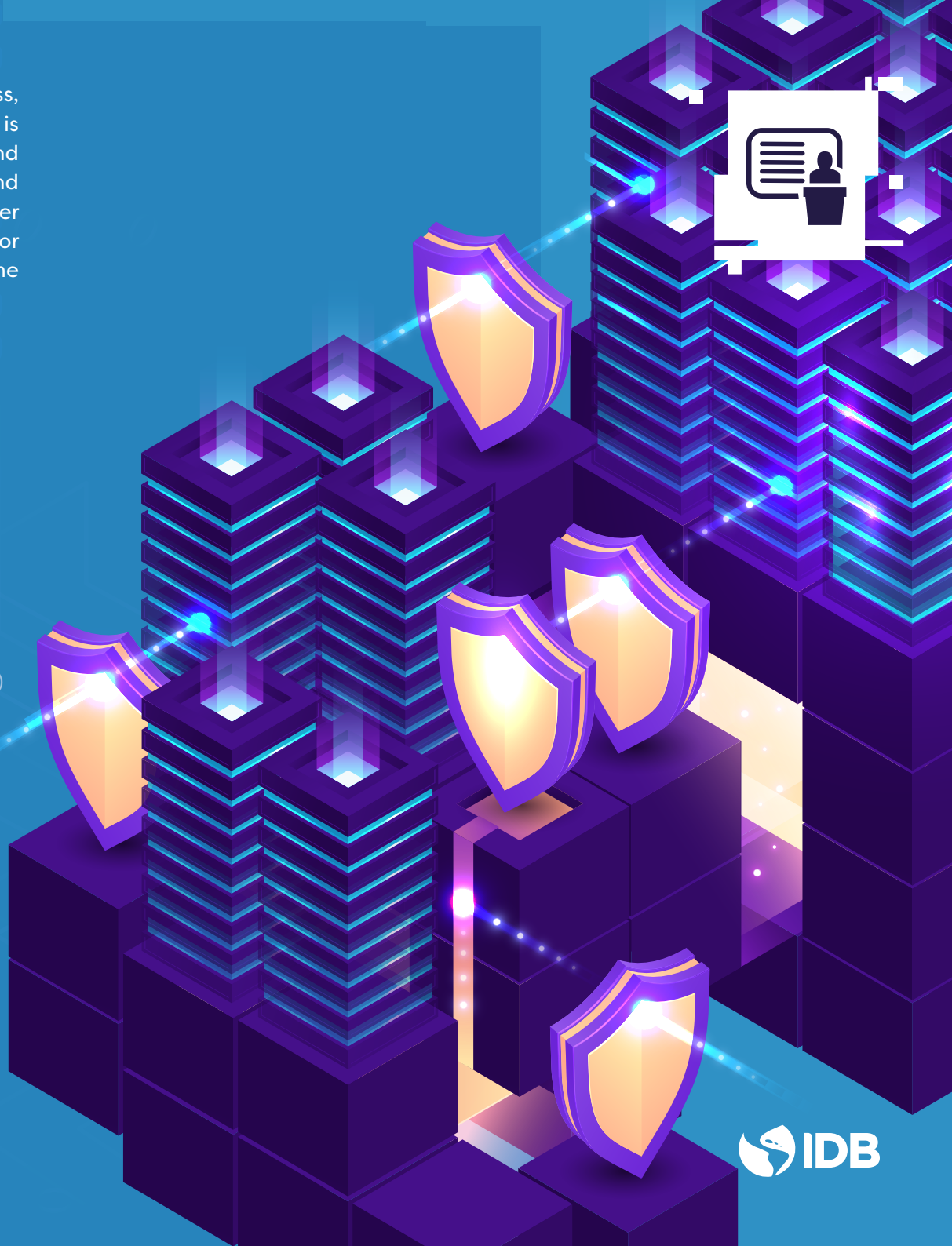
Cyberspace is a field of opportunities in terms of technological progress, connectivity, integration, and global connection to the internet. But it is also a field of threats and risks. Cyberattacks can harm organizations and inflict significant financial and image damage. To be prepared to defend against cyberthreats, an organization must master a large number of specializations, whether they are technological, organizational, or process centered. The list of documents presented below reflects the state of the collection at the time of publication of this document.

Volume A: A methodological approach

Volume B: A technical approach

- **B.01** Securing Internet of Medical Things (IoMT) Components
- **B.02** Securing Access Point Name (APN) Infrastructure
- **B.03** Hardening Computer Systems
- **B.04** Reducing Cybersecurity Risks in Video Surveillance Cameras
- **B.05** Reducing Cybersecurity Risks at the Organization's Endpoints
- **B.06** Securing Enterprise Resource Planning (ERP) Systems
- **B.07** Preparation for and Response to a Ransomware Attack in the Organization
- **B.08** Reducing Cybersecurity Risks for Industrial Control Systems (ICS)
- **B.09** Cybersecurity Risk Survey Template for Industrial Control Systems (ICS)
- **B.10** Securing Voice over Internet Protocol (VoIP) Infrastructure
- **B.11** Advanced Multi-Factor Authentication against Cybersecurity Threats
- **B.12** Major Cybersecurity Threats of Remote User Support Platforms
- **B.13** Prevention of and Response to Border Gateway Protocol (BGP) Hijacking
- **B.14** Preparation for Distributed Denial-of-Service (DDoS) Attacks
- **B.15** Reducing Cybersecurity Risks in Building Management Systems (BMS)
- **B.16** Cybersecurity through Mobile Device Management (MDM/EMM) Systems
- **B.17** Securing Managed File Transfer (MFT)
- **B.18** Cybersecurity Aspects of Commercial Message Distribution (SMS)
- **B.19** The Israeli Cyber Emergency Response Team (CERT) Principles of Operation
- **B.20** Securing Multimedia Systems
- **B.21** Integrating Principles of Cybersecurity in the Backup and Recovery Processes

Volume C: Secure software development



IDB