TLP:GREEN

CyFun®

The CyberFundamentals Framework 2025 CyFun® 2025 Key Measures

An initiative of the Centre for Cybersecurity Belgium

Belgian Cybersecurity Certification Authority

Key Measures CyFun®

		CyFun® 2023	CyFun® 2025
Total N° of Key Measures	**BASIC**	13	13
Total N° of Key Measures	**IMPORTANT**	8	9
Total N° of Key Measures	**ESSENTIAL**	7	7
Total N° of Key Measures		**28**	**29**

Printed or offline copies of this document are considered uncontrolled and may not reflect the latest revisions.
The most current version of this document is available at www.cyfun.eu

Key Measures CyFun® Basic

	CyFun® 2023		CyFun® 2025
PR.AC-1.1	Identities and credentials for authorized devices and users shall be managed.	**PR.AA-01.1**	Identities and credentials for authorized users, services, and hardware shall be managed.
PR.AC-3.2	The organization's networks when accessed remotely shall be secured, including through multi-factor authentication (MFA).	**PR.AA-03.2**	Multi-Factor Authentication (MFA) shall be used whenever possible to enhance security, especially in situations where sensitive information or critical systems are involved.
PR.AC-4.1	Access permissions for users to the organization’s systems shall be defined and managed.	**PR.AA-05.1**	Access permissions, rights, and authorisations shall be defined, managed, enforced and reviewed.
PR.AC-4.2	It shall be identified who should have access to the organization's business's critical information and technology and the means to get access.	**PR.AA-05.2**	It shall be determined who needs access to the organisation's business-critical information and technology and the means to gain access.
PR.AC-4.3	Employee access to data and information shall be limited to the systems and specific information they need to do their jobs (the principle of Least Privilege).	**PR.AA-05.3**	Access rights, privileges and authorisations shall be restricted to the systems and specific information needed to perform the tasks (the principle of Least Privilege).
PR.AC-4.4	Nobody shall have administrator privileges for daily tasks.	**PR.AA-05.4**	No one shall have administrative priviliges for routine day-to-day tasks.
PR.AC-5.1	Firewalls shall be installed and activated on all the organization's networks.	**PR.IR-01.1**	Firewalls shall be installed, configured, and actively maintained on all networks used by the organization to protect against unauthorized access and cyber threats.
PR.AC-5.2	Where appropriate, network integrity of the organization's critical systems shall be protected by incorporating network segmentation and segregation.	**PR.IR-01.2**	To safeguard critical systems, organizations shall implement network segmentation and segregation aligned with trust boundaries and asset criticality, thereby limiting threat propagation and enforcing strict access control.
PR.IP-4.1	Backups for organization's business critical data shall be conducted and stored on a system different from the device on which the original data resides.	**PR.DS-11.1**	Backups for organisation's business critical data shall be performed and stored on a different system from the device on which the original data resides.
PR.MA-1.1	Patches and security updates for Operating Systems and critical system components shall be installed.	**ID.AM-08.2**	Patches and security updates for Operating Systems and critical system components shall be installed.
PR.PT-1.1	Logs shall be maintained, documented, and reviewed.	**PR.PS-04.1**	Logs shall be maintained, documented, and monitored.
DE.AE-3.1	The activity logging functionality of protection / detection hardware or software (e.g. firewalls, anti-virus) shall be enabled, backed-up and reviewed.	**DE.AE-03.1**	The logging functionality of protection and detection tools shall be enabled. Logs shall be backed up and retained for a predefined period and regularly reviewed to identify unusual or potentially harmful activity.
DE.CM-4.1	Anti-virus, -spyware, and other -malware programs shall be installed and updated.	**DE.CM-01.2**	Anti-virus, -spyware, and other -malware programs shall be installed and updated.

	CyFun® 2023	CyFun® 2025	Changes
Total N° of Key Measures	13	13	No new Key Measures, Actionability enhancement, Rephrasing, Renumbering

Key Measures CyFun® Important

	CyFun® 2023		CyFun® 2025
ID.AM-6.1	Information security and cybersecurity roles, responsibilities and authorities within the organization shall be documented, reviewed, authorized, and updated and aligned with organization-internal roles and external partners.	**GV.RR-02.1**	Information security and Cybersecurity roles, responsibilities and authorities for employees, suppliers, customers, and partners shall be documented, reviewed, authorized, kept up to date, communicated, and coordinated internally and externally.
PR.AC-3.3	Usage restrictions, connection requirements, implementation guidance, and authorizations for remote access to the organization’s critical systems environment shall be identified, documented and implemented.	**PR.AA-03.3**	The organisation shall define, document, and implement usage restrictions, connection requirements, and authorisation procedures for remote access to its critical systems. These controls shall ensure that only approved users can connect, using secure methods, with access limited to what is necessary for their role.
PR.AC-5.3	Where appropriate, network integrity of the organization's critical systems shall be protected by (1) Identifying, documenting, and controlling connections between system components; (2) Limiting external connections to the organization's critical systems.	**PR.IR-01.3**	To ensure operational stability and security, the organisation shall, without exception, identify, document, and control connections between components of its critical systems.
PR.AC-5.4	The organization shall monitor and control connections and communications at the external boundary and at key internal boundaries within the organization's critical systems by implementing boundary protection devices where appropriate.	**PR.IR-01.4**	The organization shall implement appropriate boundary protection measures to monitor and control communications at external and key internal boundaries of its critical systems, across both IT and OT environments, to ensure secure and reliable operations.
PR.IP-1.1	The organization shall develop, document, and maintain a baseline configuration for its business-critical systems.	**PR.PS-01.1**	The organisation shall develop, document, and maintain a baseline configuration for its business-critical systems.
PR.DS-5.1	The organization shall take appropriate actions resulting in the monitoring of its critical systems at external borders and critical internal points when unauthorized access and activities, including data leakage, is detected.	**RS.MI-01.2**	The organisation shall detect unauthorised access or data leakage and take appropriate mitigation actions, including monitoring of critical systems at external boundaries and key internal points.
DE.CM-1.2	The organization shall monitor and identify unauthorized use of its business-critical systems through the detection of unauthorized local connections, network connections and remote connections.	**DE.CM-01.3**	The organisation shall monitor and identify unauthorised use of its business-critical systems through the detection of unauthorised local connections, network connections and remote connections.
RS.AN-5.1	The organization shall implement vulnerability management processes and procedures that include processing, analyzing and remedying vulnerabilities from internal and external sources.	**ID.RA-08.1**	The organisation shall establish and implement a vulnerability management plan to identify, analyse, assess, mitigate and communicate all types of vulnerabilities including in the form of a Coordinated Vulnerability Disclosure (CVD) according to applicable legal modalities.
		RS.CO-02.2	Cybersecurity incidents shall be shared with relevant external stakeholders within the timeframes defined in the Incident Response Plan, including reporting significant incidents to authorities as required by law.

	CyFun® 2023	CyFun® 2025	Changes
Total N° of Key Measures	8	9	Actionability enhancement, Rephrasing, Renumbering 1 new Key Measure: RS.CO-02.2 ➔ Ref. NIS2 for important and essential entities

Key Measures CyFun® Essential

	CyFun® 2023		CyFun® 2025
ID.SC-3.2	Contractual information security and cybersecurity’ requirements for suppliers and third-party partners shall be implemented to ensure a verifiable flaw remediation process, and to ensure the correction of flaws identified during ‘information security and cybersecurity’ testing and evaluation.	ID.AM-03-3	The organisation's network communication and external data flows shall be mapped, documented , authorised, and updated when changes occur.
ID.SC-3.3	The organization shall establish contractual requirements permitting the organization to review the ‘information security and cybersecurity’ programs implemented by suppliers and third-party partners.	GV.SC-05.2	Contractual information/cybersecurity requirements for suppliers and external partners shall be implemented to ensure a verifiable flaw resolution process and to ensure that deficiencies identified during information/cybersecurity testing and evaluation are remedied.
PR.MA-1.5	The organization shall prevent the unauthorized removal of maintenance equipment containing organization's critical system information.	GV.SC-05.3	The organisation shall establish contractual requirements permitting the organisation to review the information/cybersecurity programs implemented by suppliers and third-party partners.
PR.MA-1.6	Maintenance tools and portable storage devices shall be inspected when brought into the facility and shall be protected by anti-malware solutions so that they are scanned for malicious code before they are used on organization's systems.	ID.AM-08.7	The organisation shall prevent unauthorised removal of maintenance equipment containing critical system information of the organisation.
PR.MA-1.7	The organization shall verify security controls following hardware and software maintenance or repairs/patching and take action as appropriate.	ID.AM-08.9	Maintenance tools and portable storage devices shall be inspected as they enter the facility and shall be protected by anti-malware solutions that scan them for malicious code before they are used on the organisation's systems.
PR.PT-2.3	Portable storage devices containing system data shall be controlled and protected while in transit and in storage.	ID.AM-08.10	The organisation shall verify security controls following maintenance or repairs/patching, and take action as appropriate.
DE.AE-1.1	The organization shall ensure that a baseline of network operations and expected data flows for its critical systems is developed, documented and maintained to track events.	PR.DS-02.1	Portable storage devices containing system data shall be controlled and protected while in transit and in storage.

	CyFun® 2023	CyFun® 2025	Changes
Total N° of Key Measures	7	7	No new Key Measures, Actionability enhancement, Rephrasing, Renumbering

KEY MEASURE

CyberFundamentals IMPORTANT

GV.RR-02.1
INFORMATION SECURITY AND CYBERSECURITY ROLES, RESPONSIBILITIES AND AUTHORITIES FOR EMPLOYEES, SUPPLIERS, CUSTOMERS, AND PARTNERS SHALL BE DOCUMENTED, REVIEWED, AUTHORIZED, KEPT UP TO DATE, COMMUNICATED, AND COORDINATED INTERNALLY AND EXTERNALLY.

GOAL

To ensure all internal and external parties understand and fulfil their cybersecurity roles, responsibilities and authorities, reducing gaps, overlaps, and delays in incident response and compliance.

KEY MEASURE

CyberFundamentals ESSENTIAL

GV.SC-05.2
CONTRACTUAL INFORMATION/CYBERSECURITY REQUIREMENTS FOR SUPPLIERS AND THIRD-PARTY PARTNERS SHALL BE IMPLEMENTED TO ENSURE A VERIFIABLE FLAW RESOLUTION PROCESS, AND TO ENSURE THAT DEFICIENCIES IDENTIFIED DURING INFORMATION/CYBERSECURITY TESTING AND EVALUATION ARE REMEDIED.

GOAL

To embed enforceable requirements in supplier contracts to guarantee timely flaw remediation and resolution of cybersecurity issues identified through testing and evaluation.

KEY MEASURE

CyberFundamentals ESSENTIAL

GV.SC-05.3
THE ORGANISATION SHALL ESTABLISH CONTRACTUAL REQUIREMENTS PERMITTING THE ORGANIZATION TO REVIEW THE INFORMATION/CYBERSECURITY PROGRAMS IMPLEMENTED BY SUPPLIERS AND THIRD-PARTY PARTNERS.

GOAL

To ensure that the organization can assess and verify the information/cybersecurity practices of suppliers and third-party partners through contractual agreements.

KEY MEASURE

CyberFundamentals BASIC

DE.AE-03.1
THE LOGGING FUNCTIONALITY OF PROTECTION AND DETECTION TOOLS SHALL BE ENABLED. LOGS SHALL BE BACKED UP AND RETAINED FOR A PREDEFINED PERIOD AND REGULARLY REVIEWED TO IDENTIFY UNUSUAL OR POTENTIALLY HARMFUL ACTIVITY.

GOAL

To make sure that

- Security tools have logging turned on,
- Logs are kept for a set time,
- Logs are regularly checked to spot unusual or harmful activity.

This helps detect threats early and take action.

Examples of such tools include firewalls, antivirus software, endpoint detection, and intrusion detection systems.

KEY MEASURE

CyberFundamentals BASIC

DE.CM-01.2
ANTI-VIRUS, -SPYWARE, AND OTHER -MALWARE PROGRAMS SHALL BE INSTALLED AND UPDATED.

GOAL

To ensure that all organisational devices (IT and OT assets) are protected against malicious software through the deployment and regular updating of anti-malware tools.

KEY MEASURE

CyberFundamentals IMPORTANT

DE.CM-01.3
THE ORGANISATION SHALL MONITOR AND IDENTIFY UNAUTHORISED USE OF ITS BUSINESS-CRITICAL SYSTEMS THROUGH THE DETECTION OF UNAUTHORISED LOCAL CONNECTIONS, NETWORK CONNECTIONS AND REMOTE CONNECTIONS.

GOAL

To ensure that the organisation can detect and respond to unauthorised access or misuse of its business-critical systems. This includes identifying suspicious local, network, or remote connections that could indicate a security breach or misuse of sensitive systems.

KEY MEASURE

CyberFundamentals BASIC

ID.AM-08.2
PATCHES AND SECURITY UPDATES FOR OPERATING SYSTEMS AND CRITICAL SYSTEM COMPONENTS SHALL BE INSTALLED.

GOAL

To ensure that operating systems and critical system components are kept secure and up to date by installing patches and security updates in a timely and controlled manner.

KEY MEASURE

CyberFundamentals IMPORTANT

ID.RA-08.1
THE ORGANISATION SHALL ESTABLISH AND IMPLEMENT A VULNERABILITY MANAGEMENT PLAN TO IDENTIFY, ANALYSE, ASSESS, MITIGATE AND COMMUNICATE ALL TYPES OF VULNERABILITIES INCLUDING IN THE FORM OF A COORDINATED VULNERABILITY DISCLOSURE (CVD) ACCORDING TO APPLICABLE LEGAL MODALITIES.

GOAL

To ensure that all types of vulnerabilities are systematically identified, analysed, assessed, mitigated, and communicated through a documented vulnerability management plan. This includes handling disclosures in line with Coordinated Vulnerability Disclosure (CVD) practices and applicable legal requirements.

KEY MEASURE

CyberFundamentals ESSENTIAL

ID.AM-03.3
THE ORGANISATION'S NETWORK COMMUNICATION AND EXTERNAL NETWORK DATA FLOWS SHALL BE MAPPED, DOCUMENTED, AUTHORIZED, AND UPDATED WHEN CHANGES OCCUR.

GOAL

To ensure that external network communications are clearly understood, controlled, and monitored to reduce the risk of unauthorized access, data leakage, or service disruption across ICT and OT environments.

KEY MEASURE

CyberFundamentals ESSENTIAL

ID.AM-08.7
THE ORGANISATION SHOULD PREVENT UNAUTHORISED REMOVAL OF MAINTENANCE EQUIPMENT CONTAINING CRITICAL SYSTEM INFORMATION OF THE ORGANISATION.

GOAL

To prevent unauthorised removal of maintenance equipment that may contain critical system information, reducing the risk of data leakage or theft, especially in operational technology (OT) environments.

KEY MEASURE

CyberFundamentals ESSENTIAL

ID.AM-08.9
MAINTENANCE TOOLS AND PORTABLE STORAGE DEVICES SHALL BE INSPECTED AS THEY ENTER THE FACILITY AND SHALL BE PROTECTED BY ANTI-MALWARE SOLUTIONS THAT SCAN THEM FOR MALICIOUS CODE BEFORE THEY ARE USED ON THE ORGANISATION'S SYSTEMS.

GOAL

To prevent the introduction of malicious code into organisational systems by ensuring that all maintenance tools and portable storage devices are inspected and scanned before use.

KEY MEASURE

CyberFundamentals ESSENTIAL

ID.AM-08.10
THE ORGANISATION SHALL VERIFY SECURITY CONTROLS FOLLOWING MAINTENANCE OR REPAIRS/PATCHING, AND TAKE ACTION AS APPROPRIATE.

GOAL

To ensure that security controls remain effective after maintenance, repairs, or patching activities. In OT environments, even small configuration changes can have significant safety or operational consequences, making post-maintenance verification critical.

KEY MEASURE

CyberFundamentals BASIC

PR.AA-01.1
IDENTITIES AND CREDENTIALS FOR AUTHORISED USERS, SERVICES, AND HARDWARE SHALL BE MANAGED.

GOAL

To ensure that that identities and credentials for authorized users, services, and hardware are properly managed to prevent unauthorized access and support secure operations in both ICT and OT environments.

KEY MEASURE

CyberFundamentals BASIC

PR.AA-03.2
MULTI-FACTOR AUTHENTICATION (MFA) SHALL BE REQUIRED TO ACCESS THE ORGANISATION'S NETWORKS REMOTELY.

GOAL

To protect the organization’s networks by requiring multi-factor authentication (MFA) for all remote access, reducing the risk of unauthorized access and credential-based attacks.

KEY MEASURE

CyberFundamentals BASIC

PR.AA-05.1
ACCESS PERMISSIONS, RIGHTS AND AUTHORISATIONS SHALL BE DEFINED, MANAGED, ENFORCED AND REVIEWED.

GOAL

To ensure that access permissions, rights, and authorisations are clearly defined, properly managed, consistently enforced, and regularly reviewed to protect systems and data from unauthorised access.

KEY MEASURE

CyberFundamentals BASIC

PR.AA-05.2
IT SHALL BE DETERMINED WHO NEEDS ACCESS TO THE ORGANISATION'S BUSINESS-CRITICAL INFORMATION AND TECHNOLOGY AND THE MEANS TO GAIN ACCESS.

GOAL

To determine who requires access to the organization’s business-critical information and technology, and to define the secure means by which that access is granted.

KEY MEASURE

CyberFundamentals BASIC

PR.AA-05.3

ACCESS RIGHTS, PRIVILEGES AND AUTHORISATIONS SHALL BE RESTRICTED TO THE SYSTEMS AND SPECIFIC INFORMATION NEEDED TO PERFORM THE TASKS (THE PRINCIPLE OF LEAST PRIVILEGE).

GOAL

To ensure that access rights, privileges, and authorisations are restricted to only the systems and specific information needed to perform assigned tasks, following the principle of least privilege.

KEY MEASURE

CyberFundamentals BASIC

PR.AA-05.4
NO ONE SHALL HAVE ADMINISTRATIVE PRIVILEGES FOR ROUTINE DAY-TO-DAY TASKS.

GOAL

To prevent the use of administrative privileges for routine, day-to-day tasks, reducing the risk of misuse or exploitation by attackers.

KEY MEASURE

CyberFundamentals BASIC

PR.DS-11.1
BACKUPS FOR THE ORGANISATION'S BUSINESS-CRITICAL DATA SHALL BE PERFORMED AND STORED ON A DIFFERENT SYSTEM FROM THE DEVICE ON WHICH THE ORIGINAL DATA RESIDES.

GOAL

To ensure that business-critical data is regularly backed up and securely stored on a separate system to protect against data loss, system failure, or cyberattacks such as ransomware.

KEY MEASURE

CyberFundamentals BASIC

PR.IR-01.1
FIREWALLS SHALL BE INSTALLED, CONFIGURED, AND ACTIVELY MAINTAINED ON ALL NETWORKS USED BY THE ORGANIZATION TO PROTECT AGAINST UNAUTHORIZED ACCESS AND CYBER THREATS.

GOAL

To ensure that all networks used by the organisation are protected against unauthorised access and cyber threats through the installation, configuration, and active maintenance of firewalls.

KEY MEASURE

CyberFundamentals BASIC

PR.IR-01.2
TO SAFEGUARD CRITICAL SYSTEMS, ORGANIZATIONS SHALL IMPLEMENT NETWORK SEGMENTATION AND SEGREGATION ALIGNED WITH TRUST BOUNDARIES AND ASSET CRITICALITY, THEREBY LIMITING THREAT PROPAGATION AND ENFORCING STRICT ACCESS CONTROL.

GOAL

To limit the spread of cyber threats and enforce strict access control by implementing network segmentation and segregation based on trust boundaries and the criticality of systems.

KEY MEASURE

CyberFundamentals BASIC

PR.PS-04.1
LOGS SHALL BE MAINTAINED, DOCUMENTED, AND MONITORED.

GOAL

To ensure that logs are consistently maintained, documented, and monitored to support visibility, accountability, and early detection of anomalies or threats.

KEY MEASURE

CyberFundamentals IMPORTANT

PR.AA-03.3
THE ORGANISATION SHALL DEFINE, DOCUMENT, AND IMPLEMENT USAGE RESTRICTIONS, CONNECTION REQUIREMENTS, AND AUTHORISATION PROCEDURES FOR REMOTE ACCESS TO ITS CRITICAL SYSTEMS. THESE CONTROLS SHALL ENSURE THAT ONLY APPROVED USERS CAN CONNECT, USING SECURE METHODS, WITH ACCESS LIMITED TO WHAT IS NECESSARY FOR THEIR ROLE.

GOAL

To ensure that remote access to critical systems is tightly controlled through defined usage restrictions, secure connection methods, and formal authorisation procedures.

KEY MEASURE

CyberFundamentals IMPORTANT

PR.IR-01.3
TO ENSURE OPERATIONAL STABILITY AND SECURITY, THE ORGANISATION SHALL, WITHOUT EXCEPTION, IDENTIFY, DOCUMENT, AND CONTROL CONNECTIONS BETWEEN COMPONENTS OF ITS CRITICAL SYSTEMS.

GOAL

To maintain operational stability and security by ensuring that all connections between components of critical systems are known, documented, and actively managed.

KEY MEASURE

CyberFundamentals IMPORTANT

PR.IR-01.4
THE ORGANISATION SHALL IMPLEMENT APPROPRIATE BOUNDARY PROTECTION MEASURES TO MONITOR AND CONTROL COMMUNICATIONS AT EXTERNAL AND KEY INTERNAL BOUNDARIES OF ITS CRITICAL SYSTEMS, ACROSS BOTH IT AND OT ENVIRONMENTS, TO ENSURE SECURE AND RELIABLE OPERATIONS.

GOAL

To ensure secure and reliable operations by actively monitoring and controlling communications at key network boundaries, especially where critical systems interface with external networks or less trusted internal zones.

KEY MEASURE

CyberFundamentals IMPORTANT

PR.PS-01.1
THE ORGANISATION SHALL DEVELOP, DOCUMENT, AND MAINTAIN A BASELINE CONFIGURATION FOR ITS BUSINESS-CRITICAL SYSTEMS.

GOAL

To ensure that all business-critical systems operate in a known, secure, and approved state. A baseline configuration defines the standard setup for these systems, helping to detect unauthorized changes, enforce security policies, and support consistent operations.

KEY MEASURE

CyberFundamentals ESSENTIAL

PR.DS-02.1 PORTABLE STORAGE DEVICES CONTAINING SYSTEM DATA SHALL BE CONTROLLED AND PROTECTED WHILE IN TRANSIT AND IN STORAGE.

GOAL

To prevent unauthorised access, tampering, or loss of critical system data when portable storage devices are moved between locations or stored outside secure environments.

NEW

KEY MEASURE

CyberFundamentals IMPORTANT

RS.CO-02.2
CYBERSECURITY INCIDENTS SHALL BE SHARED WITH RELEVANT EXTERNAL STAKEHOLDERS WITHIN THE TIMEFRAMES DEFINED IN THE INCIDENT RESPONSE PLAN, INCLUDING REPORTING SIGNIFICANT INCIDENTS TO AUTHORITIES AS REQUIRED BY LAW.

GOAL

To ensure that all relevant external parties are informed about cybersecurity incidents in a timely, secure, and appropriate manner, helping to maintain trust and meet legal and contractual obligations.

KEY MEASURE

CyberFundamentals IMPORTANT

RS.MI-01.2
THE ORGANISATION SHALL DETECT UNAUTHORISED ACCESS OR DATA LEAKAGE AND TAKE APPROPRIATE MITIGATION ACTIONS, INCLUDING MONITORING OF CRITICAL SYSTEMS AT EXTERNAL BOUNDARIES AND KEY INTERNAL POINTS.

GOAL

To detect unauthorised access and data leakage in a timely manner and to take appropriate mitigation actions.

CyFun®

Thank you

CCB Certification Authority (NCCA)

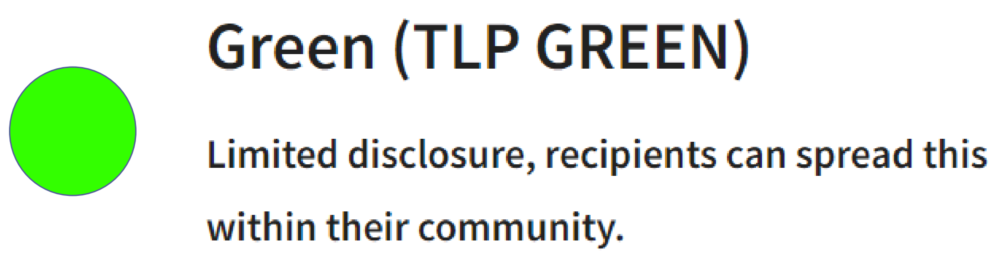
Certification@ccb.belgium.be

Centre for Cybersecurity Belgium
Rue de la Loi / Wetstraat 18 – 1000 Brussels

www.ccb.belgium.be

What does TLP Green mean?

TRAFFIC LIGHT PROTOCOL (TLP)



🟢 **Green (TLP GREEN)**

Limited disclosure, recipients can spread this within their community.

Sources may use TLP:GREEN when information is useful to increase awareness within their wider community.

Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels (e.g. websites, LinkedIn…). TLP:GREEN information may not be shared outside of the community. Note: when “community” is not defined, assume the cybersecurity/defense community.