This is a guidance box. Remove all guidance boxes after filling out the template. Items highlighted in turquoise should be edited appropriately. Items highlighted in green are examples and should be removed. After all edits have been made, all highlights should be cleared.

Insert organization logo by clicking on the placeholder to the left.

Protection against Distributed Denial of Service (DDOS) attacks Standard template

Replace <organization name> with the name of the organization for the entire document. To do so, perform the following:

- Press “Ctrl” + “H” keys simultaneously
- Enter “<organization name>” in the Find text box
- Enter your organization’s full name in the “Replace” text box
- Click “More”, and make sure “Match case” is ticked
- Click “Replace All”
- Close the dialog box.

Choose Classification

DATE	Click here to add date
VERSION	Click here to add text
REF	Click here to add text

Disclaimer

This template has been developed by the National Cybersecurity Authority (NCA) as an illustrative example that can be used by organizations as a reference and guide. This template must be customized and aligned with the <organization name>'s business and relevant legislative and regulatory requirements. This template must be approved by the head of the organization (Authorizing official) or his/her delegate. The NCA is not responsible for any use of this template as is, and it affirms that this template is solely an illustrative example.

Document Approval

Role	Job Title	Name	Date	Signature
Choose Role	<Insert job title>	<Insert individual's full personnel name>	Click here to add date	<Insert signature>

Version Control

Version	Date	Updated By	Version Details
<Insert version number>	Click here to add date	<Insert individual's full personnel name>	<Insert description of the version>

Review Table

Periodical Review Rate	Last Review Date	Upcoming Review Date
<Once a year>	Click here to add date	Click here to add date

Table of Contents

Purpose

This standard aims to define the detailed cybersecurity requirements related to Distributed Denial of Service (DDoS) attack protection for <organization name>. The ability of <organization name> to apply the controls specified in this DDoS protection standard will assist in preserving the availability, integrity and confidentiality of <organization name>'s information and assets.

The requirements in this standard are aligned with the cybersecurity requirements issued by the National Cybersecurity Authority (NCA) including but not limited to ECC-1:2018 and CSCC-1:2019, in addition to other related cybersecurity legal and regulatory requirements.

Scope

These standard covers <organization name>'s best practices in DDoS protection solution deployment and usage and applies to all assets and all personnel (employees and contractors) in <organization name>.

Standards

1	General Requirements
Objective	The DDoS protection solution must be securely deployed and used appropriately when required.
Risk Implication	Misconfiguration of DDoS protection solution may cause unavailability of business services provided to the client and internal company services.
Requirements	
1-1	DDoS protection solution must offer a service level agreement with a guaranteed time to mitigation (TTM). It is especially important when deploying as a service.

1-2	DDoS protection solution must protect both IPv4 and IPv6 stack of <organization name> network.
1-3	DDoS protection solution must have consistent application uptime and availability.
1-4	DDoS protection solution must protect networks, DNS servers, publicly accessible & hosted websites within <organization name> IT environment and individual IPs.
1-5	DDoS protection solution must have a multi-layered protection from DDoS attacks on the network and application layers, volumetric and non-volumetric attacks, as well as full coverage of SSL/TLS-based DDoS attacks.
1-6	All <organization name>'s IT administrators defined in Access Management Principles that need access to the DDoS attacks logs must have configured access to the logs database.
1-7	DDoS protection solution must be possible to be deployed in various methodologies - Table A.
1-8	All security updates to the DDoS protection solution must be installed in accordance to patch management process.
1-9	All management communication channels must be using a dedicated management network or the management network communications which is authenticated and encrypted using cryptographic modules validated in line with National Cryptography Standard and internal <organization name>'s cryptography standards. There must be protection in case of access to the managing console in DDoS as a Service deployment method.
1-10	DDoS Response and mitigation plan should be established in accordance with the relevant legislative and regulatory requirements.

1-11	<organization name> must perform periodic training for employees to ensure that they know how to choose the right mitigation service and measure training effectiveness based on reviewing the KPIs annually
2	Attack prevention
Objective	Properly configured and securely managed DDoS protection solution must prevent attempts to DDoS attack on <organization name> infrastructure.
Risk Implication	Misconfiguration of a DDoS solution may have severe consequences like legitimate traffic blocking and denial of service.
Requirements	
2-1	<organization name> must identify and protect, using DDoS protection solution, all assets available from the public network to ensure that they are capable of responding effectively to DoS/DDoS attacks.
2-2	DDoS protection solution must be tailored to <organization name>'s industry profile.
2-3	DDoS protection solution must provide reports and dashboards of prevented attacks and actions.
2-4	DDoS protection solution must offer multi-layered protection. When deployed with a web application firewall (WAF), DDoS Protection solution protects both at the network layer and at the application layer.
2-5	DDoS protection solution must use security feeds delivered by national trusted organizations like National Cybersecurity Authority (NCA).
3	Attack detection, alerting and mitigation

Objective	DDoS protection solution must detect anomalies and using filtering and limiting technique to mitigate attacks.
Risk Implication	Improper detection may easily cause malware propagation, denial of service and information leak.
Requirements	
3-1	<organization name> must define key performance indicators to track effectiveness and trends related to DDoS protection solution
3-2	DDoS protection solution must stop the spread of the DoS/DDoS and prevent further damage to the system.
3-3	DDoS protection solution must use automation to quickly mitigate arising attacks.
3-4	DDoS protection solution must deliver real-time visibility into DDoS threats with reporting and attack correlation through attack analytics or a SIEM integration.
3-5	DDoS protection solution must provide instant attack notifications.
3-6	DDoS protection solution must inform users about performed actions, rejected and mitigated attacks.
3-7	Alerts must be configured at the start and end of an attack, and over the attack's duration, using built-in attack metrics
3-8	DDoS protection solution should use machine learning and artificial intelligence in order to prevent new threats.
3-9	DDoS protection solution must be configured to send only specific logs to the central log system using syslog protocol and CEF (Common Event Format), LEEF (Log Event Extended Format) or RFC 5425 specified log format.

3-10	DDoS protection solution must attribute malicious behavior to a specific IP address and perform forensic analysis to determine how threats have moved laterally within an environment.
3-11	DDoS protection solution must constantly monitor network activity to detect traffic anomalies, such as unusual growth of network throughput or higher than usual usage of network resources.
4	Other Standards
Objective	The DDoS protection solution must be securely configured, deployed and used appropriately according to best practices and compliant to standards and relevant policies security environment.
Risk Implication	If <organization name> is not compliant with all applicable and mandatory standards and requirements, it could be exposed to severe threat rise specific for areas covers by below mentioned standards.
Requirements	
4-1	The following standards must be implemented in relevance to DDoS Solutions: 1. Identity and access management 2. Disaster recovery and backup 3. Cryptography 4. Event and audit logging 5. Physical security 6. Secure configuration and hardening 7. Event Log Management and Monitoring

Table A – DDoS protection solution deployment methodologies

Methodology	Description
DDoS Protection as a Service	Application of service providers' solutions. DDoS Protection as a Service is usually implemented by redirecting network traffic to an external scrubbing center.
On-premise (hardware)	Deployment of the solution on the <organization name>'s network, which is performed by installing the hardware in its network.
Hybrid	This methodology combines deployment as a service with on-premise to mitigate volumetric attacks as close to the source of the attack as it is possible, and mitigate application DDoS attacks on the perimeter of <organization name>'s network using the resource of Cloud/ISP scrubbing center if the DDoS attack exceed the capability of the on-prem hardware.

Roles and Responsibilities

1- **Standard Owner:** <head of the cybersecurity function>

2- **Standard Review and Update:** <cybersecurity function>

3- **Standard Implementation and Execution:** <information technology function> and <cybersecurity function>

4- **Standard Compliance Measurement:** <cybersecurity function>

Update and Review

<cybersecurity function> must review the standard at least once a year or in case any changes happen to the policy or the regulatory procedures in <organization name> or the relevant regulatory requirements.

Compliance

1- The <head of the cybersecurity function> will ensure compliance of <organization name> with this standard on a regular basis.

2- All personnel at <organization name> must comply with this standard.

3- Any violation of this standard may be subject to disciplinary action according to <organization name>'s procedures.