CYBER GUIDELINE DOCUMENT

NCSP Guideline – Internet Connections

ABSTRACT:
This guideline covers recommendations for the commissioning and use of internet connections, with a specific focus on the requirements of the Law Enforcement Community Network (LECN).

ISSUED	January 2025
PLANNED REVIEW DATE	January 2026
DISTRIBUTION	Community Security Policy Framework Members

POLICY VALIDITY STATEMENT
This guideline is due for review on the date shown above. After this date, this document may become invalid.

Cyber guideline users should ensure that they are consulting the currently valid version of the documentation.

CONTENTS

Community Security Policy Commitment

National Policing and its community members recognise that threats to policing information assets present significant risk to policing operations. National Policing and its community members are committed to managing information security and risk and maintaining an appropriate response to current and emerging threats, as an enabling mechanism for policing to achieve its operational objectives whilst preserving life, property, and civil liberties.

This guideline in conjunction with the National Policing Community Security Policy Framework and associated documents sets out National Policing recommendations for the use of internet connections for forces, especially those used to connect to LECN.

Introduction

This guidance is to assist members of the UK policing community of trust in the commissioning and operation of internet connections. This includes some specific entries for the connectivity of the Law Enforcement Community Network (LECN) as it moves to using the internet as the underlay network, rather than the PSN, allowing forces to achieve optimum levels of connection.

Not all force internet connections will be used for LECN, therefore connections may not need to apply all the recommendations of this document.

This document should be used in conjunction with the Network Security Standard which contains further controls, including mandatory ones.

Owner

National Chief Information Security Officer (NCISO).

Purpose

The purpose of this guideline is to provide members of the policing community of trust with a reference guide to help them commission and manage internet connections, especially those used for LECN.

Audience

This guidance is for staff members within National Policing and its community, who will be architecting, commissioning and managing internet connections.

Scope

1. This guidance should be considered and referenced each time a new internet connection is installed in a police force, or when a contract change is needed on an existing one.
2. This guidance should be followed by all those involved in policing networking.
3. Not all requirements in this guidance will be applicable for every internet connection used in policing but should be considered and assessed for suitability.

Requirements

Reference	Minimum requirement	Control reference	Compliance Metric
1. Commercial arrangements			
1.1	Internet connections should be "business" or "enterprise" products from a UK internet service provider (ISP), who are regulated by Ofcom, with commercial agreements in place. For "nearshore" forces, not on the mainland UK, the choice of ISP should be discussed with your Cyber Compliance Officer.	LECN Programme Requirements ISF SoGP TI1.2.9	Third Part Assurance completed on ISP. Check contracts are in place and provide sufficient coverage for the items listed in this guidance.
1.2	The ISP should support the connection with a 24/7 network operations centre, with proactive ticketing, and reporting.	LECN Programme Requirements	Check contracts are in place and provide sufficient coverage for the items listed in this guidance.
2. Bandwidth			
2.1	Each connection should each be capable of supporting the known traffic volumes which can feasibly be expected for that connection.	LECN Programme Requirements	Network monitoring of existing connections used to inform the procurement process.

Reference	Minimum requirement	Control reference	Compliance Metric
2.2	The connections should each be capable of supporting any planned growth in traffic volumes expected over the lifetime of the circuit.	LECN Programme Requirements	Network monitoring of existing connections used to inform the procurement process.
2.3	The connections should each have some capacity to handle any unplanned growth in traffic volumes.	LECN Programme Requirements	Network monitoring of existing connections used to inform the procurement process.
2.4	The connections that will be used for LECN should have the ability to support a minimum of 200Mbps of traffic.	LECN Programme Requirements	Network monitoring of existing connections used to inform the procurement process.
2.5	Avoid the use of connections with contention ratios greater than 1:1.	LECN Programme Requirements	Network monitoring of connections to check bandwidth availability.
3. Denial of service protection			
3.1	Each internet connection should have protection against denial of service (DoS) and distributed denial of service (DDoS) attacks.	LECN Programme Requirements NCSC Denial of Service (DoS) guidance	Commercial contract stating the service is in place. Contract reviews including statistics on the performance of the service.
3.2	DoS and DDoS protection should be capable of detecting and protecting against all known types of volumetric attack (for example, UDP flood and ICMP flood).	LECN Programme Requirements NCSC Denial of Service (DoS) guidance	Independent test reports showing the capabilities of the service.

Reference	Minimum requirement	Control reference	Compliance Metric
3.3	DoS and DDoS protection should have the ability to monitor and block traffic from discrete IP addresses through to whole subnets.	LECN Programme Requirements NCSC Denial of Service (DoS) guidance	Product demonstrations and assessments.
3.4	DoS and DDoS protection should include automatic and manual interventions. Any automatic interventions should be tuneable to prevent false indications (both positive and negative).	LECN Programme Requirements	Product demonstrations and assessments.
3.5	The ISP should not impose limits on the number of DoS and DDoS interventions it conducts over a given time period.	LECN Programme Requirements	Commercial contract stating the service is in place.
3.6	The ISP should provide access to a dashboard showing DoS and DDoS reports including what thresholds are set to.	LECN Programme Requirements	Product demonstrations and assessments.
3.7	The ISP should provide 24/7 access to security analysts to support DoS and DDoS attacks.	LECN Programme Requirements	Commercial contract stating the service is in place.
4. Hardware and software			
4.1	No hardware should be installed if the manufacturer has announced the end-of-life (EOL) date for the model.	LECN Programme Requirements NCSC Device Security Guidance	Asset registers. Asset lifecycle management processes. Vulnerability scanning.

Reference	Minimum requirement	Control reference	Compliance Metric
4.2	For any hardware where the EOL date has been announced, plans to replace it should be developed to ensure it is replaced before the EOL date passes.	LECN Programme Requirements NCSC Device Security Guidance	Asset lifecycle management processes.
4.3	Hardware in the critical path of a LECN internet connection should have dual power supplies, ideally powered from separate supplies.	LECN Programme Requirements	Technical design assurance processes. Data centre management processes.
4.4	Hardware in the critical path of a LECN internet connection should be protected by an uninterruptable power supply (UPS).	LECN Programme Requirements ISF SoGP PE1.4.3a	Technical design assurance processes. Data centre management processes.
4.5	Any hardware being used to connect to the provided LECN edge device should have an available port with the correct presentation for the connection to be made.	LECN Programme Requirements	Network mapping. Technical design assurance processes.
4.6	If using the same physical switch for the failover of the LECN edge devices, as used for any sharing of the internet connection, the minimum requirement is separation via VLANs with no ability for traffic to bridge the VLANs.	LECN Programme Requirements ISF SoGP HE2.1.17d	Technical design assurance processes. Security design assurance processes. Network management processes.

Reference	Minimum requirement	Control reference	Compliance Metric
5. IP addressing and name resolution			
5.1	For internet connections used for LECN, the ISP(s) must agree to advertise the LECN provided Provider Independent (PI) addressing used for the LECN underlay.	LECN Programme Requirements	Commercial contract stating the service is in place.
5.2	For domain name resolution of internet addresses, use the NCSC's Protective DNS (PDNS) service.	IAM & PS Blueprints – volume 6 2.2.3	Checking of firewall logs to ensure all DNS lookups are going to expected DNS server addresses.
6. Circuit resilience			
6.1	If one physical site has multiple internet connections that are relied upon for resilience of access to LECN, the force must ensure that the connections take separate routes, ideally to separate exchanges or points-of-presence (POP). This may require the connections are from separate ISPs.	LECN Programme Requirements ISF SoGP SR1.2.7	Commercial contract stating the service is in place.
6.2	If multiple physical sites use the same ISP and this arrangement is relied upon for resilience of access to LECN, the force must ensure that the ISP provides separation of the connections so that there is no single point of failure (i.e. the circuits do not all converge at the same exchange or POP).	LECN Programme Requirements ISF SoGP SR1.2.7	Commercial contract stating the service is in place.
6.3	If multiple physical internet connections are used, forces should consider automating the failover process, for example using dynamic	ISF SoGP SR1.2.6	Network mapping. Technical design assurance processes.

Reference	Minimum requirement	Control reference	Compliance Metric
	routing protocols, or the use of load balancers to control which proxy server is used. Care should be taken to ensure this does not result in asymmetric routing.		

Communication approach

This document will be communicated as follows:

- Internal peer review by the members of the National Cyber Policy & Standards Working Group (NCPSWG), which includes PDS and representatives from participating forces.

- Formal publication and external distribution to PDS community, police forces and associated bodies.

Measurables generated by adopting this guideline can also form part of regular cyber management reporting.

Forces should circulate this guidance internally as needed, throughout networks and IT operations teams.

Review Cycle

This guideline will be reviewed at least annually (from the date of publication) and following any major change to Information Assurance (IA) strategy, membership of the community, or an identified major change to the cyber threat landscape. This ensures IA requirements are reviewed, and that the guideline continues to meet the objectives and strategies of the police service.

Document Compliance Requirements

(Adapt according to Force or PDS Policy needs.)

Equality Impact Assessment

(Adapt according to Force or PDS Policy needs.)

Document Information

Document Location

https://knowledgehub.group/web/national-standards/policing-standards

Revision History

Version	Author	Description	Date
0.1	PDS Cyber Architects	Initial version	27/09/2024
0.2	PDS Cyber Architects	Updates following internal reviews	12/11/2024

Approvals

Version	Name	Role	Date
1.0	NCPSWG	National Cyber Policy & Standards Working Group	04/12/24

Document References

Document Name	Version	Date
ISF - Standard of Good Practice (for Information Security)	v2024	03/2024
NCSC Device Security Guidance	Web Page	06/2021
NCSC Denial of Service (DoS) Guidance	Web Page	11/2020
PDS Identity and Access Management & Productivity Services Blueprints, Volume 6	V8.4	05/2022