POLICY / PROCEDURE TITLE		DATE OF APPROVAL
Policy Against Malicious Code		February 2024
APPROVED BY	**VERSION NO.**	**VALID UNTIL**
Executive Board	2.0	February 2025

OWNER	IT Security Lead		
GROUP EXECUTIVE LEAD	Chief Information Data & Estates Officer		
DOCUMENT TYPE	Policy ☒	Group Procedure ☐	Local Procedure ☐
PURPOSE	The purpose of this policy is to provide guidance on the use of malicious code/malware across our IT network.		
APPLICABLE TO	All users who have access to NCG networks and systems.		
EQUALITY ANALYSIS COMPLETED [POLICIES ONLY]	Yes ☒	No ☐	N/A ☐
	(If EA not applicable, please explain)		
KEY THINGS TO KNOW ABOUT THIS POLICY	1. NCG has a **policy** to protect its software and information assets against malware. 2. NCG **prohibits** the use of unauthorised software on any information processing system or device it owns or operates. Software that has not been obtained in line with the procurement procedure may not be transferred or downloaded onto NCG's network via or from external networks, or on any medium, unless specific controls have been implemented. 3. NCG **requires** the installation and maintenance of anti-malware/anti-virus software on all NCG information systems and devices. All users are required to accept the NCG Acceptable Use policy and to receive appropriate training in detecting and responding to malware attacks in order to access the NCG network and services.		
EXPECTED OUTCOME	Readers are expected to understand the organisational position on Malicious Code, know their responsibilities in relation to the policy and comply with the terms of the policy.		

MISCELLANEOUS	
LINKED DOCUMENTS	• Acceptable Use Policy (AUP) • Business Continuity Plan (BCP) • Information Security Incident Management (ISIM) • Cyber Incident Response Plan (CIRP)

	• Authorising New Information Processing Facilities and Software Procedure
KEYWORDS	• Software • Malicious Code • Procurement • Virus • Malware

Equality Impact Assessment

EQUALITY IMPACT ASSESSMENT			
	Yes	**No**	**Explanatory Note if required**
EIA 1 - Does the proposed policy/procedure align with the intention of the NCG Mission and EDIB Intent Statement in Section 2?	☒	☐	The answer to this must be YES
EIA 2 - Does the proposed policy/procedure in any way impact unfairly on any protected characteristics below?	☐	☒	
Age	☐	☒	The answer to this must be NO
Disability / Difficulty	☐	☒	The answer to this must be NO
Gender Reassignment	☐	☒	The answer to this must be NO
Marriage and Civil Partnership	☐	☒	The answer to this must be NO
Race	☐	☒	The answer to this must be NO
Religion or Belief	☐	☒	The answer to this must be NO
Sex	☐	☒	The answer to this must be NO
Sexual Orientation	☐	☒	The answer to this must be NO
EIA3 - Does the proposed policy/processes contain any language/terms/references/ phrasing that could cause offence to any specific groups of people or individuals?	☐	☒	The answer to this must be NO
EIA4 - Does the policy/process discriminate or victimise any groups or individuals?	☐	☒	The answer to this must be NO
EIA 5 - Does this policy/process positively discriminate against any group of people, or individuals?	☐	☒	The answer to this must be NO
EIA 5 - Does this policy/process include any positive action to support underrepresented groups of people, or individuals?	☐	☒	The answer to this could be yes or no as positive action is lawful. However, an explanation must be provided for clarity.
EIA 6 - How do you know that the above is correct?	This policy is required as part of regulatory commitments and is not open to negotiation.		

1. GENERAL POLICY STATEMENT

1.1 NCG acts to protect the integrity of its software and its other information assets against the introduction of malicious code (malware).

1.2 NCG formally prohibits the use on any information processing system or device it owns or operates, of any software whose procurement was not carried out through NCG procurement procedure, taking into account the requirements of the 'Authorising New Information Processing Facilities and Software Procedure'.

1.3 Software that has not been obtained in line with the 'Authorising New Information Processing Facilities and Software Procedure', and any other files or folders, may not be transferred or downloaded onto NCG's network via or from external networks, or on any medium (including CD-ROMs, Portable Storage Devices, USB sticks etc.), including during maintenance and emergency procedures, unless specific controls have been implemented.

1.4 NCG formally prohibits the use of mobile code except where that mobile code has been authorised for use by NCG in a specification. An example of acceptable uses of mobile code include business critical website scripts that deliver Java script functionality, following approval.

1.5 Monitoring, detecting and deleting unauthorised software is a requirement of the NCG Infrastructure team and disciplinary action may be taken against anyone who introduces malicious software or applications on to NCG's networks, systems or services.

1.6 NCG acts to identify and patch software and system vulnerabilities in order to reduce the risk of malware attacks.

1.7 The installation and maintenance of anti-malware/anti-virus software on all NCG information systems and devices is mandatory.

1.8 In order to access the NCG network and services all users are required to accept the NCG Acceptable Use policy and to receive appropriate training in detecting and responding to malware attacks.

1.9 Business continuity plans are required to make specific provision whilst recovering from malware attacks. The Cyber Incident Response Plan should be used as guidance for recovery from such attacks.

1.10 The Information Security Incident Management procedure is required to make specific provision for responding to malware attacks.

1.11 Management is required to take adequate steps to ensure that it is aware of and can respond to changes in the malware threat environment.

2. STATEMENT ON POLICY IMPLEMENTATION

2.1 Upon approval, this policy will be uploaded to the policy portal and communicated to staff via The Business Round-Up

3. STATEMENT ON EQUALITY AND DIVERSITY

3.1 NCG is committed to providing equality of opportunity. Further details or our aims and objectives are outlined in our Equality Diversity Inclusion and Belonging Strategy.

3.2 This policy has been assessed to identify any potential for adverse or positive impact on specific groups of people protected by the Equality Act 2010 and does not discriminate either directly or indirectly. In applying this policy, we have considered eliminating unlawful discrimination, promoting equality of opportunity and promoting good relations between people from diverse groups.

4. STATEMENT ON CONSULTATION

4.1 This policy has been reviewed in consultation with members of the Information and Data Services team and subsequently with members of the Policy Review Council as part of the policy review and approval process.

VERSION CONTROL				
Version No.	**Documentation Section/Page No.**	**Description of Change and Rationale**	**Author/Reviewer**	**Date Revised**
1.0		Annual review and update	N/A	07/05/15
1.1		Annual review and update	N/A	18/07/16
1.2		Review and update for new legislation	N/A	02/05/18
1.3		Annual review and update	Director IDES	05/09/22

2.0	Full Document	Annual Review and update of template format	IT Security Lead	17/01/24