OpenUK Response to the UK Government's Call for Views on the Code of Practice for Enterprise Connected Device Manufacturers

Principle 1: Provide Updates, Securely
Question: Do you agree with the inclusion of this principle in the proposed Code of Practice for Enterprise Connected Device Security?
Guidelines:

- 1.1: The manufacturer shall publish the minimum period for which the device will receive security updates
- 1.2: The device shall verify that an update is from a trusted source and that it wasn't altered during transit
- 1.3: The device should use best-practice cryptography to support secure updates
- 1.4: The manufacturer shall publish a policy defining the regularity and frequency of updates
- 1.5: Device updates shall be provided in response to critical vulnerabilities and incidents
- 1.6: Updates shall be manageable and flexible for administrators or other authorised entities (either users or other devices or services) across device fleets
- 1.7: Details of updates shall be published that state which publicly known vulnerabilities have been mitigated

OpenUK Recommendation: Strongly Agree.

Written Response:
We support this principle as essential for modern device lifecycle security. However, the combination of publishing, cryptographic verification, and fleet management may be too ambitious for all vendors.

Principle 2: Support Appropriate Authentication
Guidelines:

- 2.1: The device shall only grant access to a user following successful authentication
- 2.2: The device shall support authentication with other devices, services and networks
- 2.3: After initial setup, any credentials shall either be defined by the user or be unique to the device
- 2.4: Pre-installed credentials shall be generated using a mechanism that reduces the risk of automated attacks
- 2.5: All authentication protocols used on the device shall adhere to current best practice
- 2.6: The device should support hardware-backed methods of authentication
- 2.7: Device identity should be bound to the physical device in a non-exportable fashion

OpenUK Recommendation: Strongly Agree

Written Response:
This principle addresses credential security with both baseline (unique credentials) and advanced (hardware-backed identity) protections. It aligns with both ETSI EN 303 645 and zero-trust standards.

Principle 3: Protect Data at Rest and in Transit
Guidelines:

- 3.1: The device should support the encryption of all user data at rest
- 3.2: When active, the device should support encryption of data
- 3.3: The device shall protect sensitive data in transit using a secure transport mechanism or application layer protocol
- 3.4: The device shall use best-practice cryptography when protecting data
- 3.5: Long-term cryptographic secret keys shall be securely generated and stored
- 3.6: An authenticated and authorised user shall be able to delete sensitive data

- 3.7: Data should be compartmentalised, with appropriate access control

OpenUK Recommendation: Strongly Agree

Written Response:
The guidelines reflect modern expectations around data minimization, encryption, and access control. We strongly support these guidelines and recommend secure deletion methods (e.g., cryptographic wipe) be emphasized.

Principle 4: Maintain Device Integrity
Guidelines:

- 4.1: The firmware and OS shall only be modifiable using authorised update mechanisms
- 4.2: The device shall support pre-OS boot security
- 4.3: The device should have a framework for runtime integrity protection
- 4.4: The device shall provide documented exploit mitigation capabilities
- 4.5: Integrity of device health data should be maintained
- 4.6: The device can be physically hardened

OpenUK Recommendation: Strongly Agree

Written Response:
This principle is critical. We recommend minor clarifications (e.g., secure enclaves, IMA framework), but overall the guidelines are aligned with risk mitigation for tampering and long-term exploitation.

Principle 5: Ensure Transparency of Device Health
Guidelines:

- 5.1: The manufacturer shall provide documentation of its definition of device health
- 5.2: During runtime, the health of the device shall be available locally
- 5.3: During runtime, the health of the device should be available remotely
- 5.4: The device should have a boot attestation process
- 5.5: The device should have a runtime attestation process that provides regular or continuous monitoring

OpenUK Recommendation: Strongly Agree

Written Response:
This principle encourages measurable trust and supports zero-trust architectures. However, “device health” definitions vary. A standard format or guidance is needed to ensure interoperability.

Principle 6: Permit Only Trusted Software
Guidelines:

- 6.1: It shall be possible to restrict the use of software based on trust
- 6.2: Access to trusted tools shall be configurable per user
- 6.3: Restrictions on executing software should be configurable based on users or groups

OpenUK Recommendation: Strongly Agree

Written Response:
This prevents unverified or malicious code from executing. Clarification is needed on how enterprises may add third-party trusted software beyond manufacturer defaults.

Principle 7: Minimise the Privilege and Reach of Applications
Guidelines:

- 7.1: Devices shall limit application access to privacy features until permission is granted
- 7.2: Software shall run with the lowest permissions needed
- 7.3: OS should support a granular permissions model
- 7.4: Software should be compartmentalised
- 7.5: Devices should only include software/hardware required for functionality

OpenUK Recommendation: Strongly Agree

Written Response:
This principle strongly aligns with least privilege and sandboxing practices. We recommend emphasizing permission revocation and secure defaults.

Principle 8: Constrain the Use of All Device Interfaces
Guidelines:

- 8.1: Services and their interfaces shall be clearly documented
- 8.2: Interfaces should be user/organisation-configurable
- 8.3: Devices shall have a runtime mechanism to identify services/endpoints
- 8.4: Manufacturer shall state interface misuse mitigations
- 8.5: These mitigations should be enabled by default
- 8.6: Interfaces should be disableable if not required

OpenUK Recommendation: Strongly Agree

Written Response:
We agree and strongly encourage explicit guidance on physical interfaces like debug ports. Interfaces should be off by default where not needed.

Principle 9: Allow Robust Device Management
Guidelines:

- 9.1: Devices shall be configurable locally and remotely
- 9.2: Admins shall be able to enforce configuration
- 9.3: Devices should support automated onboarding
- 9.4: Devices can use open standards for management
- 9.5: Configurations should be exportable/importable

OpenUK Recommendation: Strongly Agree

Written Response:
We support this strongly and recommend confirming secure configuration backup handling and compatibility with open standards (e.g., MQTT, TR-369).

Principle 10: Provide Logging, Alerting, and Monitoring
Guidelines:

- 10.1: Security events shall be viewable locally or remotely
- 10.2: Devices shall support IoC application to traffic
- 10.3: Devices shall securely forward logs
- 10.4: Reliable time sources shall be used for accurate logging
- 10.5: Manufacturer shall document log formats
- 10.6: Devices shall log network connections
- 10.7: Devices shall alert on significant changes in state

OpenUK Recommendation: Strongly Agree

Written Response:
Logs must be secure, exportable, and aligned with standard formats. We recommend clarifying whether 10.2 implies IDS functionality or metadata-level observability.

Principle 11: Enable Recovery to a Known Good State
Guidelines:

- 11.1: Devices shall be capable of being reset into a known state
- 11.2: It should be possible to remotely wipe the device
- 11.3: It should be possible to lock the device remotely
- 11.4: Linking data with enterprise repositories enables backup/sync

OpenUK Recommendation: Strongly Agree

Written Response:
We support secure reset with remote lock/wipe. Recommend confirming secure reset partition mechanisms and linkage to remote attestation for trust re-establishment.

Suggested Principle: Vulnerability Disclosure
Recommendation: Recommend Inclusion
Written Response:
We recommend a new principle requiring public vulnerability disclosure channels and secure development practices aligned to ISO 29147. This closes the loop with secure updates (Principle 1).

Question: Should Government Encourage Greater Cybersecurity in Enterprise Connected Devices?
OpenUK Recommendation: Strongly Agree
Written Response:
Government intervention is required due to a lack of existing incentives and market failure in secure-by-default practices.

Question: Are Enterprise Risks Sufficiently Distinct to Justify a Separate Code?
OpenUK Recommendation: Agree
Written Response:
Enterprise devices are high-value targets, and the need for management, attestation, and

auditability go well beyond consumer expectations.

Question: Would You Support Option 1: A Voluntary Pledge?
OpenUK Recommendation: Agree
Written Response:
A voluntary pledge is a good starting point, but should include a core minimum set of principles, public transparency, and a roadmap to escalation if needed.