Security Requirement		☆1 Security Requirement	[Ref.] Existing schemes/documents of other countries	[Ref.] Existing domestic schemes/documents
Category	Requirement			
1. No universal default passwords	1-1. Where passwords are used and in any state other than the factory default, all passwords shall be unique per device or defined by the user.	✓	[ETSI EN 303 645]5.1-1 M C (1) [UK: PSTI Act]SCHEDULE 1: 1-(2) [US: NISTIR 8425]Interface Access Control 1-b [Singapore: CLS][*]5.1-1 [IEC 62443-4-2]CR1 5, CR1.7	[MIC: Ordinance Concerning Terminal Facilities, etc.]Article 34-10 (2) [CCDS Certification]1-1 Access Control and Authentication [Mandatory] 2), 1-1-2 Change of credentials [Mandatory] 2) [BMSec]IA-2 b)-2), e)-2) 2 2) [JISEC-C0755]FMT_IPWD_EXT
1. No universal default passwords	1-2. Where pre-installed unique passwords are used, these shall be sufficiently randomized against automated attacks.	✓	[ETSI EN 303 645]5.1-2 M C (2) [UK: PSTI Act]SCHEDULE 1: 1-(3) [Singapore: CLS][＊]5.1-2 [IEC 62443-4-2]CR1.7	[MIC: Ordinance Concerning Terminal Facilities, etc.]Article 34-10 (2) [CCDS Certification]1-1 Access Control and Authentication [Mandatory] 2) [JISEC-C0755]FMT_IPWD_EXT
1. No universal default passwords	1-3. Authentication mechanisms used to authenticate users against the product shall use technologies that reduce the assumed risks appropriate to the properties of the product usage etc.	✓	[ETSI EN 303 645]5.1-3 M [UK: PSTI Act]SCHEDULE 1: 1-(3) [US: NISTIR 8425]Interface Access Control2-b [EU: CRA]ANNEX I 1.(3)(b) [Singapore: CLS][＊]5.1-3 [IEC 62443-4-2]CR1 5	[MIC: Ordinance Concerning Terminal Facilities, etc.]Article 34-10 (1) [CCDS Certification]1-1 Access Control and Authentication [Mandatory] 4), 1-2 Data Protection[Mandatory] 3) [RBSS]Certification Standard for Security Camera 5.2.12 (2), Certification Standard for Digital Recorder（Security Uses）　5.2.12 (2) [JISEC-C0755]FIA_UAU, FMT_SMR
1. No universal default passwords	1-4. For user authentication against the product, the products shall provide to the user or an administrator a simple mechanism to change the authentication value used.	✓	[ETSI EN 303 645]5.1-4 M C (8) [Singapore: CLS][＊]5.1-4 [IEC 62443-4-2]CR1 5	[CCDS Certification]1-1-2 Change of credentials [Mandatory] 1) [BMSec]IA-2 [RBSS]Certification Standard for Digital Recorder（Security Uses）　5 2.12 (2) [JISEC-C0755]FMT_IPWD_EXT
1. No universal default passwords	1-5. When the device is not a constrained device, it shall have a mechanism available which makes brute-force attacks on authentication mechanisms via a network impracticable.	✓	[ETSI EN 303 645]5.1-5 M C (5) [EU: CRA]ANNEX I 1.(3)(b) [Singapore: CLS][＊]5.1-5 [IEC 62443-4-2]CR1.11	[MIC: Ordinance Concerning Terminal Facilities, etc.]Article 34-10 (1) [CCDS Certification]1-1 Access Control and Authentication [Mandatory] 3) [BMSec]IA-3 [JISEC-C0755]FIA_AFL
2. Managing vulnerability reports	2-1. The manufacturer shall make a vulnerability disclosure policy publicly available. This policy shall include, at a minimum: • contact information for the reporting of issues; and • information on timelines for: 1) initial acknowledgement of receipt; and 2) status updates until the resolution of the reported issues.	✓	[ETSI EN 303 645]5.2-1 M [UK: PSTI Act]SCHEDULE 1: 2-(2), 2-(3) [US: NISTIR 8425]Information & Query Reception1, 1-a, 1-b, Product Education & Awareness [EU: CRA]ANNEX I 2.(5), ANNEX I 2 (6), ANNEX II 1, ANNEX II 2 [Singapore: CLS][＊]5 2-1 [IEC 62443-4-1]DM-1	[CCDS Certification]2-1 Contact point and security support system [Mandatory] 1) [BMSec] FR-1
2. Managing vulnerability reports	2-2. The manufacturer shall act for disclosed vulnerabilities in a timely manner.		[ETSI EN 303 645]5.2-2, R [US: NISTIR 8425]Documentation 1-g [EU: CRA]ANNEX I 2.(7), Article 10 12 [IEC 62443-4-1]DM-2, DM-3, DM-4	[BMSec] FR-2
2. Managing vulnerability reports	2-3. The manufacturer shall continually monitor for, identify and rectify security vulnerabilities within products and services they sell, produce, have produced and services they operate during the defined support period.		[ETSI EN 303 645]5.2-3 R [EU: CRA]ANNEX I 1.(3)(k) [IEC 62443-4-1]DM-2	
2. Managing vulnerability reports	2-4. The manufacturer shall report to the designated organization within a specified period of time the fact that a vulnerability in the product has been exploited, if known to the designated organization.		[EU: CRA]Article 11 1, Article 11 2 , Article 11 4, Article 11 7 [IEC 62443-4-1]SG-3	
2. Managing vulnerability reports	2-5. The manufacturer must continually update their security problem management processes.		[IEC 62443-4-1]DM-6	
3. Keep software updated	3-1. Particular software components included in products shall be updateable.	✓	[ETSI EN 303 645]5.3-1 R [US: NISTIR 8425]Software Update 1 [EU: CRA]ANNEX I 2.(8) [Singapore: CLS][＊＊＊]CK-LP-03 [IEC 62443-4-1]SM-6, SUM-1 [IEC 62443-4-2]CR4 3, CR3.10 EDR3.10, HDR3.10 NDR 3.10	[CCDS Certification]1-3 Software Update [Mandatory] 1) [Recommended] 1) [BMSec]PT-1 [JISEC-C0755]FMT_SMF
3. Keep software updated	3-2. When the device is not a constrained device, it shall have an update mechanism for the secure installation of updates.	✓	[ETSI EN 303 645]5.3-2 M C (5) [US: NISTIR 8425]Software Update 1 [Singapore: CLS][＊]5 3-2	[MIC: Ordinance Concerning Terminal Facilities, etc.]Article 34-10 (3) [CCDS Certification]1-3 Software Update [Mandatory] 1) [Recommended] 1) [BMSec]PT-1 b)-3) [JISEC-C0755]FMT_SMF
3. Keep software updated	3-3. When the product implements an update mechanism, the update shall be simple for the user to apply.	✓	[ETSI EN 303 645]5.3-3 M C (12) [EU: CRA]ANNEX I 2.(8) [Singapore: CLS][＊]5 3-3 [IEC 62443-4-1]SUM-4	[MIC: Ordinance Concerning Terminal Facilities, etc.]Article 34-10 (3) [BMSec]PT-1 b)-4), e)-1) [JISEC-C0755]FMT_SMF
3. Keep software updated	3-4. Automatic mechanisms shall be used for software updates.		[ETSI EN 303 645]5.3-4 R C (12) [US: NISTIR 8425]Software Update 2 [EU: CRA]ANNEX I 1.(3)(k)	[BMSec]PT-1 b)-4), e)-1) [JISEC-C0755]FMT_SMF
3. Keep software updated	5-3. The product shall check after initialization, and then periodically, whether security updates are available.		[ETSI EN 303 645]5.3-5 R C (12) [US: NISTIR 8425]Information Dissemination 1a [EU: CRA]ANNEX I 1.(3)(k)	[BMSec]PT-1 b)-4), e)-1) [JISEC-C0755]FMT_SMF
3. Keep software updated	3-6. If the product supports automatic updates and/or update notifications, these shall be enabled in the initialized state and configurable so that the user can enable, disable, or postpone installation of security updates and/or update notifications.		[ETSI EN 303 645]5.3-6 R C (9, 12)	[CCDS Certification]1-3 Software Update [Recommended] 4) [BMSec]PT-1 b)-4), e)-1) [JISEC-C0755]FMT_SMF
3. Keep software updated	3-7. When the product implements an update mechanism, the product shall use best practice cryptography to facilitate secure update mechanisms.	✓	[ETSI EN 303 645]5.3-7 M C (12) [US: NISTIR 8425]Software Update 1 [Singapore: CLS][＊]5 3-7 [IEC 62443-4-2]CR4 3	[CCDS Certification]1-3 Software Update [Recommended] 2) [JISEC-C0755]FMT_SMF
3. Keep software updated	3-8. When the product implements an update mechanism, security updates shall be timely.	✓	[ETSI EN 303 645]5.3-8 M C (12) [EU: CRA]ANNEX I 2.(2), ANNEX I 2 (7), ANNEX I 2.(8) [Singapore: CLS][＊]5 3-8 [IEC 62443-4-1]SUM-5	[CCDS Certification]2-1 Contact point and security support system [Mandatory] 2) [BMSec]PT-1 b)-4), e)-1) [JISEC-C0755]FMT_SMF
3. Keep software updated	3-9. The product shall verify the authenticity and integrity of software updates.		[ETSI EN 303 645]5.3-9 R C (12) [EU: CRA]ANNEX I 1.(3) (E) [IEC 62443-4-1]SM-6 [IEC 62443-4-2]CR4 3, CR3.2 SAR3.2, EDR3 2 HDR3 2 NDR3.2	[CCDS Certification]1-3 Software Update [Recommended] 1) [BMSec]PT-1 [JISEC-C0755]FMT_SMF

Security Requirement		☆1 Security Requirement	[Ref.] Existing schemes/documents of other countries	[Ref.] Existing domestic schemes/documents
Category	Requirement			
3. Keep software updated	3-10. Where updates are delivered over a network interface, the product shall verify the authenticity and integrity of each update via a trust relationship.	✓	[ETSI EN 303 645]5.3-10 M (11,12) [EU: CRA]ANNEX I 1.(3)(e) [Singapore: CLS][＊]5 3-10 [IEC 62443-4-1]SM-6 [IEC 62443-4-2]CR3.1, CR3.2 SAR3.2, EDR3 2 HDR3 2 NDR3.2	[CCDS Certification]1-3 Software Update [Recommended] 1) [JISEC-C0755]FMT_SMF
3. Keep software updated	3-11. The manufacturer shall publish, in an accessible way that is clear and transparent to the user, the defined support period.		[ETSI EN 303 645]5.3-14 R C (3,4) [US: NISTIR 8425]Information Dissemination 1	
3. Keep software updated	3-12. For constrained devices that cannot have their software updated, the device shall be isolable.		[ETSI EN 303 645]5.3-15 R C (3,4) [IEC 62443-4-2]CR2 6, CR5.1	
3. Keep software updated	3-13. For constrained devices that cannot have their software updated, the device shall be the hardware replaceable.		[ETSI EN 303 645]5.3-15 R C (3,4)	
3. Keep software updated	3-14. The model designation of the products shall be clearly recognizable, either by labelling on the product or via a physical interface.	✓	[ETSI EN 303 645]5.3-16 M [US: NISTIR 8425]Information Dissemination 2 [EU: CRA]ANNEX II 3 [Singapore: CLS][＊]5 3-16	
3. Keep software updated	3-15. Machine-readable software bill of materials (SBOM) containing software identification information, component information, etc. shall be prepared.		[EU: CRA]ANNEX I 2.(1) [Singapore: CLS][＊＊＊]CK-LP-06	[BMSec] CM-1
4. Securely store sensitive parameters	4-1. Sensitive security parameters in the product's storage shall be stored securely by the product.	✓	[ETSI EN 303 645]5.4-1 M [US: NISTIR 8425]Data Protection 1, Interface Access Control 2-a [Singapore: CLS][＊＊]5.4-1 [IEC 62443-4-2]CR1 5, CR1.9, CR1.14, CR3 8, CR4.1, CR3.12 EDR3.12 HDR3.12 NDR3.12, CR3.13 EDR3.13 HDR3.13 NDR3.13	[CCDS Certification]1-2 Data Protection[Mandatory] 1) 3) [JISEC-C0755]FMT_MTD
4. Securely store sensitive parameters	4-2. Where a hard-coded unique per device identity is used in a product for security purposes, it shall be implemented in such a way that it resists tampering by means such as physical electrical or software.		[ETSI EN 303 645]5.4-2 M C (10) [Singapore: CLS][＊＊]5.4-2 [IEC 62443-4-2]CR1 5, CR3.11 EDR3.11 HDR3.11 NDR3.11	
4. Securely store sensitive parameters	4-3. Hard-coded critical security parameters in product software source code shall not be used.		[ETSI EN 303 645]5.4-3 M [Singapore: CLS][＊＊]5.4-3	
4. Securely store sensitive parameters	4-4. Any critical security parameters used for integrity and authenticity checks of software updates and for protection of communication with associated services in product software shall be unique per device and shall be produced with a mechanism that reduces the risk of automated attacks against classes of devices.		[ETSI EN 303 645]5.4-4 M [Singapore: CLS][＊＊]5.4-4 [IEC 62443-4-1]SM-8 [IEC 62443-4-2]CR3 8	[CCDS Certification]1-3 Software Update [Recommended] 1) 2)
5. Communicate securely	5-1. The product shall use best practice cryptography to communicate securely.	✓	[ETSI EN 303 645]5.5-1 M [US: NISTIR 8425]Data Protection 3 [EU: CRA]ANNEX I 1.(3)(c) [Singapore: CLS][＊＊]5 5-1 [IEC 62443-4-2]CR3.1, CR4.3	[CCDS Certification]1-2 Data Protection[Mandatory] 2), 1-4-1 Wi-Fi authentication method [Mandatory] 1), 1-4-2 Bluetooth vulnerability countermeasures [Mandatory] 1) [BMSec]TP-1
5. Communicate securely	5-2. The product shall use reviewed or evaluated implementations to deliver network and security functionalities, particularly in the field of cryptography.		[ETSI EN 303 645]5.5-2 R [US: NISTIR 8425]Data Protection 1 [EU: CRA]ANNEX I 2.(3) [Singapore: CLS][＊＊＊]CK-LP-02 [IEC 62443-4-1]SD-3 [IEC 62443-4-2]CR1 8, CR1.9, CR1.14, CR3.12 EDR3.12 HDR3.12 NDR3.12, CR3.13 EDR3.13 HDR3.13 NDR3.13	[CCDS Certification]1-2 Data Protection [Recommended] 1) 2)
5. Communicate securely	5-3. Cryptographic algorithms and primitives shall be updateable.		[ETSI EN 303 645]5.5-3 R	[JISEC-C0755]FMT_SMF
5. Communicate securely	5-4. Access to product functionality via a network interface in the initialized state shall only be possible after authentication on that interface.		[ETSI EN 303 645]5.5-4 R [US: NISTIR 8425]Interface Access Control 1-c, 2-b, 2-c [EU: CRA]ANNEX I 1.(3)(b) [IEC 62443-4-2]CR1.1, CR1.6 NDR1.6, CR1.12, CR2.1 CR1.13 NDR1.13 CR2.2 CR2.12	[RBSS]Certification Standard for Digital Recorder（Security Uses） 5 2.12 (2)
5. Communicate securely	5-5. Product functionality that allows security-relevant changes in configuration via a network interface shall only be accessible after authentication. The exception is for network service protocols that are relied upon by the product and where the manufacturer cannot guarantee what configuration will be required for the product to operate.	✓	[ETSI EN 303 645]5.5-5 M [EU: CRA]ANNEX I 1.(3)(b) [Singapore: CLS][＊＊]5 5-5 [IEC 62443-4-2]CR1 6 NDR1.6, CR2.12, CR6.1	[CCDS Certification]1-1 Access Control and Authentication [Mandatory] 4), 1-1-1 Disabling of TCP/UDP ports [Recommended] 2), 1-3 Software Update [Recommended] 3) [BMSec]IA-1, MT-1 [RBSS]Certification Standard for Security Camera 5.2.12 (2)-4, Certification Standard for Digital Recorder（Security Uses） 5.2.12 (2)-4 [JISEC-C0755]FAU_UID
5. Communicate securely	5-6. Critical security parameters shall be encrypted in transit, with such encryption appropriate to the properties of the technology, risk and usage.		[ETSI EN 303 645]5.5-6 R [EU: CRA]ANNEX I 1.(3)(c) [IEC 62443-4-1]SM-8 [IEC 62443-4-2]CR1 5 CR3.1 CR4.3	[RBSS]Certification Standard for Security Camera 5.2.12 (2), Certification Standard for Digital Recorder（Security Uses） 5.2.12 (2)
5. Communicate securely	5-7. The product shall protect the confidentiality of critical security parameters that are communicated via remotely accessible network interfaces.	✓	[ETSI EN 303 645]5.5-7 M [EU: CRA]ANNEX I 1.(3)(c) [Singapore: CLS][＊＊]5 5-7 [IEC 62443-4-2]CR3.1, CR4.3	[CCDS Certification]1-2 Data Protection[Mandatory] 2), 1-4-1 Wi-Fi authentication method [Mandatory]
5. Communicate securely	5-8. The manufacturer shall follow secure management processes for critical security parameters that relate to the product.		[ETSI EN 303 645]5.5-8 M [Singapore: CLS][＊＊]5 5-8, [＊＊＊]CK-LP-09 [IEC 62443-4-2]CR1 3 CR1.4	
5. Communicate securely	5-9. The product installed at the zone boundary shall implement functions to monitor and control communications.		[IEC 62443-4-2]CR5 2 NDR5 2	
5. Communicate securely	5-10. A function to detect tampering shall be implemented in all communications between products. If tampering is detected, actions such as notification to the user shall be performed.		[EU: CRA]ANNEX I 1.(3)(d)	[JISEC-C0755]FPT_ITI
6. Minimize exposed attack surfaces	6-1. All unused network physical interfaces and logical interfaces shall be disabled.	✓	[ETSI EN 303 645]5.6-1 M [US: NISTIR 8425]Interface Access Control 1-a [EU: CRA]ANNEX I 1.(3)(h) [Singapore: CLS][＊＊]5 6-1 [IEC 62443-4-2]CR7.7	[CCDS Certification]1-1-1 Disabling of TCP/UDP ports [Mandatory] 1) [BMSec]NI-1, VA-1, VA-2, VA-3
6. Minimize exposed attack surfaces	6-2. In the initialized state, the network interfaces of the product shall minimize the unauthenticated disclosure of security-relevant information.		[ETSI EN 303 645]5.6-2 M [US: NISTIR 8425]Interface Access Control 2-a [Singapore: CLS][＊＊]5 6-2 [IEC 62443-4-2]CR1.10	[CCDS Certification]1-1-1 Disabling of TCP/UDP ports [Mandatory] 2), 1-4-2 Bluetooth vulnerability countermeasures [Mandatory] 2)

Security Requirement		☆1 Security Requirement	[Ref.] Existing schemes/documents of other countries	[Ref.] Existing domestic schemes/documents
Category	Requirement			
6. Minimize exposed attack surfaces	6-3. Device hardware shall not unnecessarily expose physical interfaces to attack.		[ETSI EN 303 645]5.6-3 R [US: NISTIR 8425]Interface Access Control 1-a [EU: CRA]ANNEX I 1.(3)(h) [IEC 62443-4-2]CR2.13 EDR2.13, HDR2.13 NDR2.13, CR7.7, CR5.3 NDR5.3	[CCDS Certification]1-4-3 USB access control [Mandatory] 1) [Recommended] 1) 2) [BMSec]VA-2 [RBSS]Certification Standard for Security Camera 5.2.12 (2)-4, Certification Standard for Digital Recorder（Security Uses） 5.2.12 (2)-4
6. Minimize exposed attack surfaces	6-4. Where a debug interface is physically accessible, it shall be disabled in software.		[ETSI EN 303 645]5.6-4 M C (13) [EU: CRA]ANNEX I 1.(3)(h) [Singapore: CLS][＊＊]5 6-4 [IEC 62443-4-2]CR2.13 EDR2.13, HDR2.13 NDR2.13, CR7.7	[CCDS Certification]1-4-3 USB access control [Mandatory] 1) [BMSec]VA-3 [RBSS]Certification Standard for Security Camera 5.2.12 (2)-4, Certification Standard for Digital Recorder（Security Uses） 5.2.12 (2)-4
6. Minimize exposed attack surfaces	6-5. The manufacturer shall only enable software services that are used or required for the intended use or operation of the product.		[ETSI EN 303 645]5.6-5 R [Singapore: CLS][＊＊＊]CK-LP-05 [IEC 62443-4-2]CR7.7	
6. Minimize exposed attack surfaces	6-6. Code shall be minimized to the functionality necessary for the service/product to operate.		[ETSI EN 303 645]5.6-6 R [Singapore: CLS][＊＊＊]CK-LP-02, [＊＊＊]CK-LP-05 [IEC 62443-4-1]SI-1, SI-2	
6. Minimize exposed attack surfaces	6-7. Software shall run with least necessary privileges, taking account of both security and functionality.		[ETSI EN 303 645]5.6-7 R [IEC 62443-4-2]CR2.4 SAR2.4, EDR2.4 HDR2.4, NDR2.4 ﾓﾊﾞｲﾙｺｰﾄﾞ CR7.7	[RBSS]Certification Standard for Digital Recorder（Security Uses） 5 2.12 (2)
6. Minimize exposed attack surfaces	6-8. The product shall include a hardware-level access control mechanism for memory.		[ETSI EN 303 645]5.6-8 R	
6. Minimize exposed attack surfaces	6-9. The manufacturer shall follow secure development processes for software deployed on the product.		[ETSI EN 303 645]5.6-9 R [EU: CRA]Article 10 9 [IEC 62443-4-1]SM-7	[CCDS Certification]1-4-2 Bluetooth vulnerability countermeasures [Mandatory] 3) [BMSec]CM-1
6. Minimize exposed attack surfaces	6-10. Only third-party components that have been secured through penetration testing and/or code review shall be implemented.		[EU: CRA]Article 10 4, ANNEX I 1.(1), Artice 10 2 [Singapore: CLS][＊＊＊]CK-LP-03 [IEC 62443-4-1]SM-9 SM-10	
7. Ensure software integrity	7-1. The product shall verify its software using secure boot mechanisms.		[ETSI EN 303 645]5.7-1 R [EU: CRA]ANNEX I 1.(3)(e) [IEC 62443-4-1]SM-6 [IEC 62443-4-2]CR1 2, CR3.4, CR3.14 EDR3.14, HDR3.14 NDR3.14	[CCDS Certification]1-3 Software Update [Recommended] 1)
7. Ensure software integrity	7-2. If an unauthorized change is detected to the software, the product shall alert the user and/or administrator to the issue and shall not connect to wider networks than those necessary to perform the alerting function.		[ETSI EN 303 645]5.7-2 R [US: Cybersecurity State Awareness 1 [EU: CRA]ANNEX I 1.(3)(g) [IEC 62443-4-1]SM-6 [IEC 62443-4-2]CR3.7 CR6.2	
8. Ensure that personal data is secure	8-1. The confidentiality of personal data transiting between a device and a service, especially associated services, shall be protected, with best practice cryptography.		[ETSI EN 303 645]5.8-1 R [EU: CRA]ANNEX I 1.(3)(c) [IEC 62443-4-2]CR4 3	[CCDS Certification]1-2 Data Protection[Mandatory] 2) [RBSS]Certification Standard for Security Camera 5.2.12 (2)
8. Ensure that personal data is secure	8-2. The confidentiality of sensitive personal data communicated between the device and associated services shall be protected, with cryptography appropriate to the properties of the technology and usage.		[ETSI EN 303 645]5.8-2 M [EU: CRA]ANNEX I 1.(3)(c) [Singapore: CLS][＊＊]5 8-2 [IEC 62443-4-2]CR4 3	[CCDS Certification]1-2 Data Protection[Mandatory] 2)
8. Ensure that personal data is secure	8-3. All external sensing capabilities of the product shall be documented in an accessible way that is clear and transparent for the user.		[ETSI EN 303 645]5.8-3 M [Singapore: CLS][＊＊]5 8-3	
9. Resilience to outages	9-1. Resilience shall be built into the products and services, taking into account the possibility of outages of data networks and power.	✓	[ETSI EN 303 645]5.9-1 R [EU: CRA]ANNEX I 1.(3)(f) [IEC 62443-4-2]CR7.1, CR7.3	[MIC: Ordinance Concerning Terminal Facilities, etc.]Article 34-10 (4) [CCDS Certification]1-1 Access Control and Authentication [Mandatory]⑤
9. Resilience to outages	9-2. The product shall remain operating and locally functional in the case of a loss of network access and shall recover cleanly in the case of restoration of a loss of power.		[ETSI EN 303 645]5.9-2 R [EU: CRA]ANNEX I 1.(3)(f) [IEC 62443-4-2]CR7.1, CR7.4, CR7.5	
9. Resilience to outages	9-3. The product shall connect to networks in an expected, operational and stable state and in an orderly fashion, taking the capability of the infrastructure into consideration.		[ETSI EN 303 645]5.9-3 R [EU: CRA]ANNEX I 1.(3)(f) [IEC 62443-4-2]CR2.7, CR7.1, CR7.2	
9. Resilience to outages	9-4. Anti-abuse mechanisms such as access control and/or authentication shall be used to mitigate the impact of incidents.		[EU: CRA]ANNEX I 1.(3)(i), Artice 10 2, ANNEX I 1.(1) [IEC 62443-4-2]CR2.9 CR2.10 CR3.6	
10. Examine and protect system telemetry data	10-1. If telemetry data is collected from devices and services, such as usage and measurement data, it shall be examined for security anomalies.		[ETSI EN 303 645]5.10-1 R C (6) [US: Cybersecurity State Awareness 1 [EU: CRA]ANNEX I 1.(3)(j) [IEC 62443-4-2]CR2 8, CR2.11	[CCDS Certification]3-1 Audit log recording [Recommended] 1) 2) 3), 3-1-1 Time management function [Recommended] 1) [RBSS]Certification Standard for Security Camera 5.2.12 (2), Certification Standard for Digital Recorder（Security Uses） 5.2.12 (2) [JISEC-C0755]FMT_MTD_FAU_GEN
10. Examine and protect system telemetry data	10-2. Telemetry data shall be protected by mechanisms such as data encryption and access control.		[IEC 62443-4-2]CR3.9	[JISEC-C0755]FAU_STG
11. Delete user data	11-1. The user shall be provided with functionality such that user data can be erased from the product in a simple manner.	✓	[ETSI EN 303 645]5.11-1 M [US: NISTIR 8425]Data Protection 2 [Singapore: CLS][＊＊]5.11-1 [IEC 62443-4-2]CR4 2	[CCDS Certification]1-2-1 Data erasure function [Mandatory] 1) [BMSec]MT-2 [JISEC-C0755]FMT_MTD
11. Delete user data	11-2. The consumer shall be provided with functionality on the product such that personal data can be removed from associated services in a simple manner.		[ETSI EN 303 645]5.11-2 R [US: NISTIR 8425]Data Protection 2 [IEC 62443-4-2]CR4 2	[BMSec]MT-2, DP-1 [JISEC-C0755]FMT_MTD
11. Delete user data	11-3. Users shall be given clear instructions on how to delete their personal data.		[ETSI EN 303 645]5.11-3 R [US: NISTIR 8425]Data Protection 2, Product Education & Awareness 1-a [IEC 62443-4-1]SG-4	[CCDS Certification]2-3 Provision of information to users [Mandatory] 5) [BMSec]MT-2, DP-1
11. Delete user data	11-4. Users shall be provided with clear confirmation that personal data has been deleted from services, devices and applications.		[ETSI EN 303 645]5.11-4 R [IEC 62443-4-1]SG-4	
12. Make installation and maintenance of devices easy	12-1. Installation and maintenance of the product shall involve minimal decisions by the user and shall follow security best practice on usability.		[ETSI EN 303 645]5.12-1 R	[CCDS Certification]1-1-1 Disabling of TCP/UDP ports [Recommended] 1) [JISEC-C0755]FMT_MOF
12. Make installation and maintenance of devices easy	12-2. The manufacturer shall provide users with guidance on how to securely set up their product.		[ETSI EN 303 645]5.12-3 R [US: NISTIR 8425]Product Education & Awareness 1-a [EU: CRA]ANNEX I 1.(2) ANNEX I 1.(3)(a)	[BMSec]PR-1
12. Make installation and maintenance of devices easy	12-3. The manufacturer shall provide users with guidance on how to check whether their product is securely set up.		[US: NISTIR 8425]Product Configuration 1 [IEC 62443-4-2]CR1 5	

Security Requirement		☆1 Security Requirement	[Ref.] Existing schemes/documents of other countries	[Ref.] Existing domestic schemes/documents
Category	Requirement			
12. Make installation and maintenance of devices easy	12-4. The capability to restore the product to its secure default configuration settings by the user and administrator shall be implemented.		[US: NISTIR 8425]Product Configuration 2 [EU: CRA]ANNEX I 1.(3)(a)	[BMSec]MT-2
12. Make installation and maintenance of devices easy	12-5. The ability to apply configuration settings to components such as hardware, software, or firmware shall be implemented.		[US: NISTIR 8425]Product Configuration 3 [IEC 62443-4-2]CR1 5	
13. Validate input data	13-1. The product software shall validate data input via user interfaces or transferred via Application Programming Interfaces (APIs) or between networks in services and devices.		[ETSI EN 303 645]5.13-1 M [US: NISTIR 8425]Interface Access Control 2-a [EU: CRA]ANNEX I 1.(3)(e) [Singapore: CLS][＊＊]5.13-1 [IEC 62443-4-1]SVV-1 [IEC 62443-4-2]CR3 5	[CCDS Certification]1-4-4 Injection countermeasures [Mandatory] 1)
14. Protect personal data securely	14-1. The manufacturer shall provide consumers with clear and transparent information about what personal data is processed, how it is being used, by whom, and for what purposes, for each product and service. This also applies to third parties that can be involved, including advertisers.		[ETSI EN 303 645]6.1 M [US: NISTIR 8425]Product Education & Awareness 1-a [Singapore: CLS][＊＊]6.1	
14. Protect personal data securely	14-2. Where personal data is processed on the basis of consumers' consent, this consent shall be obtained in a		[ETSI EN 303 645]6.2 M C (7) [Singapore: CLS][＊＊]6 2	
14. Protect personal data securely	14-3. Consumers who gave consent for the processing of their personal data shall have the capability to withdraw it at any time.		[ETSI EN 303 645]6.3 M [Singapore: CLS][＊＊]6 3	
14. Protect personal data securely	14-4. If telemetry data is collected from devices and services, the processing of personal data shall be kept to the minimum necessary for the intended functionality.		[ETSI EN 303 645]6.4 R C (6) [EU: CRA]ANNEX I 1.(3)(e)	
14. Protect personal data securely	14-5. If telemetry data is collected from devices and services, consumers shall be provided with information on what telemetry data is collected, how it is being used by whom and for what purposes.		[ETSI EN 303 645]6.5 M C (6) [US: NISTIR 8425]Product Education & Awareness 1-a [Singapore: CLS][＊＊]6 5	
15. Make products identifiable	15-1. The product shall be uniquely identifiable by users and administrators.		[US: NISTIR 8425]Asset Identification 1 [EU: CRA]ANNEX II 3 [IEC 62443-4-2]CR1 2	[CCDS Certification]1-1 Access Control and Authentication [Mandatory] 1)
15. Make products identifiable	15-2. An inventory management mechanism shall be implemented for the product and the capability to manage connected product components.		[US: NISTIR 8425]Asset Identification 2 [IEC 62443-4-2]CR7 8	
16. Identify and test threats	16-1. A product shall be developed based on a threat analysis of the product functionalities.		[IEC 62443-4-1]SR-2, SI-1	
16. Identify and test threats	16-2. Multiple security functions shall be implemented based on the results of threat analysis.		[IEC 62443-4-1]SD-2	
16. Identify and test threats	16-3. A penetration testing shall be performed on the product.		[Singapore: CLS][＊＊＊]CK-LP-02, [＊＊＊]CK-LP-07 [IEC 62443-4-1]SVV-1, SVV-3, SM-11, SVV-4	
17. Provide information on products	17-1. Information on the security of the product shall be provided in the specified language to the specified entity.		[EU: CRA]Article 10 7, Article 10 8, Article 10 13, Article 20 2, Article 23 4 [Singapore: CLS][＊＊＊]CK-LP-04 [IEC 62443-4-1]DM-5	[BMSec]FR-2
17. Provide information on products	17-2. The manufacturer shall provide users with guidance on how to securely set up, use and dispose of their products.	✓	[ETSI EN 303 645]5.12-2 R [US: NISTIR 8425]Documentation 1-a, 1-d, Product Education & Awareness 1-a, Information Dissemination 2 [EU: CRA]ANNEX II 4, ANNEX II 9 [IEC 62443-4-1]SUM-2	[CCDS Certification]2-3 Provision of information to users [Mandatory] 1) [BMSec]PT-1, TP-1
17. Provide information on products	17-3. The manufacturer shall inform the user in a recognizable and apparent manner that a security update is required together with information on the risks mitigated by that update.	✓	[ETSI EN 303 645]5.3-11 R C (12) [US: NISTIR 8425]Information Dissemination 1c 1d 1e [EU: CRA]ANNEX I 2.(4), ANNEX I 2 (8) [IEC 62443-4-1]SUM-2	[CCDS Certification]2-3 Provision of information to users [Mandatory] 2) [BMSec]FR-2
17. Provide information on products	17-4. The product shall notify the user when the application of a software update will disrupt the basic functioning of the device.		[ETSI EN 303 645]5.3-12 R C (12) [US: NISTIR 8425]Information Dissemination 1 [EU: CRA]ANNEX I 2.(8) [IEC 62443-4-1]SUM-2 SUM-3	[JISEC-C0755]FMT_SMF
17. Provide information on products	17-5. The manufacturer shall provide the user with a specified procedure for disposing of the product.	✓	[US: NISTIR 8425]Product Education & Awareness 1-c [IEC 62443-4-1]SG-4	[CCDS Certification]2-3 Provision of information to users [Mandatory]⑤ [BMSec]DP-1
17. Provide information on products	17-6. The manufacturer shall provide information on the product, including design, manufacturing, and evaluation results, to the user in a specified manner.		[US: NISTIR 8425]Documentation 1-b [EU: CRA]Article 10 3, Article 10 11, Article 24 1, Article 24 2, Article 24 3, Article 24 4, ANNEX V 5 [IEC 62443-4-1]SG-1	
17. Provide information on products	17-7. The manufacturer shall provide the user with information on how to maintain the product in the specified manner.		[US: NISTIR 8425]Product Education & Awareness 1-b [IEC 62443-4-1]SG-5, SG-3, SG-6	[JISEC-C0755]FAU_SAR
17. Provide information on products	17-8. The manufacturer shall publish, in an accessible way that is clear and transparent to the user, the defined support period.	✓	[ETSI EN 303 645]5.3-13 M [UK: PSTI Act]SCHEDULE 1: 3-(2), 3-(3), 3-(4) [US: NISTIR 8425]Product Education & Awareness 1-d, 1-e, Information Dissemination 1b [EU: CRA]ANNEX II 6, ANNEX II 7, ANNEX II 8 [Singapore: CLS][＊]5 3-13 [IEC 62443-4-1]SG-3	[CCDS Certification]2-3 Provision of information to users [Mandatory] 4) [JISEC-C0755]FPT_SMT
17. Provide information on products	17-9. The manufacturer shall provide information to the user in a specified manner before an event leading to the cessation of operations.		[EU: CRA]Article 10 14	
17. Provide information on products	17-10. The manufacturer shall provide the user with information in a specified manner regarding product usage that may pose a security risk.	✓	[US: NISTIR 8425]Documentation 1-d [EU: CRA]ANNEX II 5 [IEC 62443-4-1]SG-3 SR-1	[CCDS Certification]2-3 Provision of information to users [Mandatory] 1) 3) [BMSec]PR-1
17. Provide information on products	17-11. The manufacturer shall provide guidance to the user on how to test security functions implemented in the product in a specified manner.		[IEC 62443-4-2]CR3 3	
18. Documentation	18-1. The manufacturer shall document data on the means used to meet the security requirements.		[EU: CRA]Article 20 1, Article 23 1 [Singapore: CLS][＊＊＊]CK-LP-01 [IEC 62443-4-1]SM-1, SM-12, SR-3, SR-4, SG-2 [IEC 62443-4-2]CR3 2 SAR3 2 EDR3.2 HDR3.2 NDR3 2	[CCDS Certification]2-2 Product document management [Mandatory] 1)
18. Documentation	18-2. The manufacturer shall continually update the prepared documentation within a specified period of time.		[EU: CRA]Article 23 2 [IEC 62443-4-1]SM-13, SR-5, SG-7	[CCDS Certification]2-2 Product document management [Mandatory] 1)

Security Requirement		☆1 Security Requirement	[Ref.] Existing schemes/documents of other countries	[Ref.] Existing domestic schemes/documents
Category	Requirement			
18. Documentation	18-3. The manufacturer shall document additional information about the product (e g., software versions that affect the intended use and compliance with the basic requirements, photographs of the product's appearance, evaluation results, etc.).		[US: NISTIR 8425]Documentation 1-d, Information Dissemination 2 [EU: CRA]Article 20 3, Article 23 3, ANNEX IV 1, ANNEX IV 2, ANNEX IV 3, ANNEX IV 4, ANNEX IV 7, ANNEX IV 8, ANNEX V 1, ANNEX V 3, ANNEX V 6 [IEC 62443-4-1]SUM-3	
18. Documentation	18-4. The manufacturer shall document information regarding the design, development, production and vulnerability response processes for the product.		[US: NISTIR 8425]Documentation 1-d, 1-e, 1-f, Information Dissemination 2 [EU: CRA]ANNEX V 2, ANNEX V 7 [Singapore: CLS][＊＊＊]CK-LP-02 [IEC 62443-4-1]SM-1 SD-1 SD-4	[CCDS Certification]2-2 Product document management [Mandatory] 1)
18. Documentation	18-5. A justification shall be recorded for each recommendation in the present document that is considered to be not applicable for or not fulfilled by the product.		[ETSI EN 303 645]4.1 [US: NISTIR 8425]Documentation 1-c [EU: CRA]ANNEX V 4 [IEC 62443-4-1]SM-3, SM-5, SI-1 [IEC 62443-4-2]CR2.12	[CCDS Certification]2-2 Product document management [Mandatory] 1)
18. Documentation	18-6. The manufacturer shall document security information about their products discovered by developers or provided by third parties and update their risk assessments.		[EU: CRA]Article 10 5 [Singapore: CLS][＊＊＊]CK-LP-08	
18. Documentation	18-7 The manufacturer shall document the laws and regulations with which the product must comply. The manufacturer shall also document the product life, operating costs and support period.		[US: NISTIR 8425]Documentation 1-a [EU: CRA]ANNEX IV 5, ANNEX IV 6 [IEC 62443-4-1]SUM-1	[CCDS Certification]2-2 Product document management [Mandatory] 1)
18. Documentation	18-8. The manufacturer shall document the requirements and considerations for product maintainers.		[US: NISTIR 8425]Documentation 1-e [IEC 62443-4-1]SVV-5	
18. Documentation	18-9. The manufacturer shall adopt a process to identify organizational roles and responsible parties during the product life cycle.		[EU: CRA]Article 20 4 [IEC 62443-4-1]SM-2	
18. Documentation	18-10. The manufacturer shall provide training to its employees aimed at acquiring security expertise.		[IEC 62443-4-1]SM-4	

*The Security Requirements (1-1 to 2-3, 3-1 to 3-14, 4-1 to 5-8, 6-1 to 6-9, 7-1 to 9-3, 10-1, 11-1 to 12-2, 13-1 to 14-5, 17-2 to 17-4, 17-8, 18-5) within this document are extracted from the ETSI EN 303 645 ©ETSI 2020. All rights reserved.

*Republished courtesy of the National Institute of Standards and Technology.