EBU

OPERATING EUROVISION AND EURORADIO

R 143

CYBERSECURITY RECOMMENDATION FOR MEDIA VENDORS' SYSTEMS, SOFTWARE & SERVICES

RECOMMENDATION

Version 2.4

Geneva
March 2024

Document History

EBU Committee	TC	
Drafting Group	MCS Group	
First published	March 2016	
Revised	11/20	V. 2.1 new version with attached spreadsheet
	04/21	V. 2.2 Major edit (Annexes A & B & Spreadsheet)
	03/22	V. 2.3 Editorial corrections and minor adjustments
	03/24	V. 2.4 Software as a Service introduced (New Annex C) updated Spreadsheet (Appendix 1)

Publication Keywords: Security, Services, Infrastructure, Broadcasting, IP, Appliance, Software, Software as a Service, SaaS, Cloud, Application, Cyber, Security Controls Assertation, Vendor, Vulnerabilities, Authentication, Password, Encryption, Certificate, PKI, Keys, Log, Incident.

Acknowledgement

EBU technical publications are the work of experts from EBU Members, Associate Members and third parties consisting of international standards bodies, industry partners, academic institutions and independent consultants.

Their contribution to EBU technical publications is a very generous act by the individuals concerned and by their employers. The EBU appreciates their efforts and thanks them most sincerely.

This document was developed from an ARD recommendation, and it has been produced with the assistance of the following entities:

EBU Members: Norbert Gust (WDR), Jörg Scheiblhofer (ORF), Yoann Duval (FTV), Mark O'Herlihy (RTE), Alvaro Martin Santos (RTVE), Rainer Jochem (ARD), Marco Bellaccini (RAI).

EBU Project Manager: Lucille Verbare.

Cybersecurity Recommendation for media vendors' systems, software & services

Recommendation

The EBU, considering that

1. Media companies increasingly employ third parties to provision their systems, software and services.
2. Production workflows and infrastructures are rapidly migrating to generic IT technologies.
3. Cyberthreats (e.g., malware and ransomware) are increasingly easy to perform and are continuously evolving.
4. Connected media devices still tend to have a low security threshold inherited from the era of non-connected broadcast media.

Recommends that media companies:

1. Apply the safety security safeguards set out in R 143 Security Controls Assertation[1] and associated guidance when planning and designing their systems, software and services.
2. Require potential vendors of systems, software and services to declare their ability to comply with R 143 Security Controls Assertation (by completing columns A & B) and associated guidance, when responding to tenders or requests for technology. In this context, media companies can optionally use column F to indicate their priorities with respect to individual requirements. A suggested best practice prioritisation is provided in Column E, with the following categorization:
   - "[P1]" designation represents critical provisions for the overall cyber security.
   - "[P2]" designation recognizes important recommendations.
   - "[P3]" designation represents best-practice arrangements.
3. Define their minimal vendor system acceptance level based on this Recommendation with full awareness of the potential risks.

[Annex A, B & C & the Security Controls Assertion spreadsheet complete this Recommendation]

[1] The Security Controls Assertation is a part of this Recommendation. It is an Excel spreadsheet that may be downloaded from the publication page of this Recommendation. **Appendix 1** reproduces the spreadsheet for information only.

Spreadsheet completion guidelines

Definitions

Product:	The Product, service, system or software being provided by the Organisation to the Customer. Product may designate an Appliance or a SaaS.
SaaS:	A software product that users connect to over the internet. It is hosted on servers or in the cloud, managed by the Vendor. It is delivered under a subscription model.
Appliance:	A Hardware with Operating System and embedded Software. It has to be hosted by Customer.
Organisation/Vendor:	The potential Vendor (including appointed sub-contractors) providing the Product, service, system or software.
Customer:	The entity that uses (purchases) a Product from your Organisation

Annex A corresponds to elements related to the Vendor's Security Management System, that needs to be completed by all Vendors in **Excel Worksheet A** of the Security Controls Assertation spreadsheet.

Vendors must then either:

- Refer to **Annex B** and complete **Excel Worksheet B** if their Product is a Media Appliance, or
- Refer to **Annex C and complete Excel Worksheet C** if their product is SaaS.

Please read all Annexes carefully as they will assist you in correctly completing the spreadsheet.

Annex D reproduces the Security Controls Assertation spreadsheet for convenience of referencing. It must not be used for data submissions, which should only be made in the Excel spreadsheet that may be downloaded from the publication page of this Recommendation.

Annex A: Vendor Information - Security Management System

[Information to assist with completion of Worksheet A of the Spreadsheet]

IS. Vendor ISMS

IS-01 Cyber security policy

A documented Cyber Security Policy (or set of policies) should be in place and approved by senior management [P1]

An information security policy is the foundation of an Organisation's security programme. It should set out how the Organisation protects information assets, considering:

> **Confidentiality:** the protection of information from unauthorised access;
>
> **Integrity:** ensuring that information is complete and accurate and hasn't been tampered with, altered or damaged in an unauthorised way;
>
> **Availability:** information is available to the right people when it is needed.

The policy should be approved and signed off by senior management to demonstrate their commitment to the Organisation's security programme.

Cyber security policies should be kept up to date and effectively communicated to all relevant personnel. [P1]

Policies should be reviewed regularly to make sure that they are suitable, adequate and effective for the Organisation.

They should be communicated regularly to everyone that needs to see them. This should be in a way that is relevant and understandable by the intended reader, and they should be easy to access.

The Organization should be certified against recognised security standards and frameworks. [P2]

There are a number of recognised cyber security frameworks and standards (including but not limited to): ISO27001, National Institute of Standards & Technology (NIST), Cloud Security Alliance (CSA), European Union Agency for Cybersecurity (ENISA), Content Delivery & Security Association (CDSA), Motion Picture Association (MPA), and Bundesamt für Sicherheit in der Informationstechnik (BSI).

If your Organisation is certified, you should provide evidence of the certification as part of the completion of the R 143 Security Controls Assertation.

IS-02 Effective cyber security organisation

All cyber security roles and responsibilities should be assigned and communicated to relevant personnel. [P2]

Cyber security roles and responsibilities should be assigned in line with the cyber security policy.

There should be a named Chief Information Security Officer (CISO) or appointed person who has overall responsibility for cyber security within the Organisation. [P1]

The CISO or appointed person should be of sufficient seniority within the Organisation and have relevant expertise and experience to be able to carry out the role effectively.

Cyber security awareness training and education should be provided to all employees (including contractors) as is relevant to their role. [P2]

Training should include at a minimum: information protection and security, password and user account security, legal and regulatory (e.g. GDPR).

IS-03 Audit plan

The Organisation should have audit procedures in place that ensure periodic review of the suitability and effective operation of its security controls framework. [P2]

Regular reviews should be carried out to ensure that the Organisation's approach to cyber security is continually being assessed for its effectiveness and suitability and that any areas identified for improvement or change are addressed.

OS. Operational Security

OS-01 Technical security analysis

Regular technical security analysis such as penetration or vulnerability testing of the Product or service should be performed. [P1]

Vulnerability scans are automated tests that identify vulnerabilities in a system or application. Penetration testing is more in depth than a vulnerability scan and can be used to identify weaknesses as well as exploit them.

System components, processes and software should be tested frequently to ensure that security of Customer information is maintained. This is especially important when significant changes are made to infrastructure or internet-facing services.

OS-02 Vulnerability management

A vulnerability management process should be in place to keep track of identified vulnerabilities and patches that may fix them. [P1]

A vulnerability management process should be in place that demonstrates to customers how frequently vulnerability testing is carried out and how patching is managed and implemented to fix any identified weaknesses.

The process should ensure that potential vulnerabilities within the Product stack are identified (e.g., if running an Oracle DB then Oracle security bulletins should be subscribed to) and there should be a release process to patch security issues for Customers in line with this.

There should be a vulnerability disclosure policy, or process in place for the responsible reporting of vulnerabilities. [P2]

Having a vulnerability disclosure policy/process helps to reduce the risk of an incident occurring. It allows a reasonable time for a Vendor to provide a vulnerability patch before it is publicly disclosed.

The Vendor should implement and follow the Common Vulnerabilities and Exposures (CVE) vulnerability management process for vulnerabilities identified in its own code and systems. [P2]

The CVE process ensures transparent communication and vulnerability management. It ensures each vulnerability has a permanent public reference, enabling customers to make informed decisions when prioritizing product updates and deployments in the future. It demonstrates that the vendor is committed to not only securing its products, but also to transparency and accountability regarding vulnerabilities.

It is expected that a Vendor will comply with EBU R 160.

The media vendor should release information immediately in the event any security vulnerability in its product(s) (own code or third-party code) becomes known. [P1]

Reporting of vulnerabilities is covered in section IM. Incident Management.

A Security Level Agreement should be put in place, which should include a specification of the maximum time to deliver patches to fix vulnerabilities, depending on their criticality and risk associated to the Product when used by the Customer. [P1]

OS-03 Product lifecycle

The Product lifecycle should be clearly defined, and patches and updates should be made available throughout that lifecycle, including for all third-party components embedded in Product. [P1]

The Product or service lifecycle should be clearly defined so that the Customer is aware of key dates. Patches and updates should be made available to ensure that security can be maintained throughout the lifecycle of the Product or service, from implementation to decommission. The media vendor shall support the security updates for all third-party components used, including the operating system platform and runtime environments used.

The Vendor should also support the upgrade of the software components of the system (OS, DBMS, Application Server etc.) if any of these components becomes unsupported.

OS-04 Product/software delivery

A secure process should be in place for the delivery of products, software or services. [P2]

The Vendor should provide physical and digital security controls for the delivery process of Products, software or services. These security controls may include:

- encrypted USB keys;
- Digitally signed files;
- delivery through secure protocols;
- encrypted software packages; and

- hash value checking.

OS-05 Customer Maintenance

Maintenance and Remote support to Customers should be provided securely. [P1]

If Customer support for the Product is done remotely, it should be provided securely, including, but not limited to:

- Use of a Virtual Private Network (VPN) using multi-factor authentication (MFA).
- Ensuring that remote support accounts are only enabled for the duration of the troubleshooting activity.
- All troubleshooting activity should be logged and reviewed.

OS-06 Separation of Production and non-Production

Production and non-Production environments should be kept separate. [P2]

Development, test and Production facilities should be separated to reduce the risk of unauthorised access or changes to the operational environment.

SD. Secure Development

SD-01 Development lifecycle

Security should be designed into and implemented through the whole lifecycle of Product development. [P2]

There should be a policy or equivalent documentation in place which outlines the secure process for the development of software or systems.

The development lifecycle should include as a minimum:

- a risk assessment/threat modelling process;
- secure design/architecture review;
- documented secure coding guidelines and industry good practice (e.g., OWASP) that are applied and kept up to date;
- mandatory test stages/security gates;
- secure code analysis where the source code and/or compiled versions of code are analysed to help find security flaws; and
- code cleaning to ensure that there is no test code remaining from the development process in the final version.

SD-02 Training

Development staff should be trained in the latest secure coding principles and industry good practice. [P2]

Development staff should receive regular training and continuous development to ensure they keep up to date with the latest secure coding principles and industry good practice.

SD-03 Source-Code

Access to proprietary program source-code should be restricted and is strictly controlled. [P2]

Proprietary program source-code should be protected, and access strictly controlled to prevent introducing unauthorised functionality, unintentional changes and to maintain confidentiality where there are intellectual property implications.

IM. Incident Management

IM-01 Incident response

A documented incident response and crisis management process/procedure should be in place, that is regularly reviewed and kept up to date. [P1]

Security incident response responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security incidents. This includes having a clear outline of responses to different attack scenarios and clear escalation routes.

The process should also include a post-incident review so that appropriate action can be taken to prevent the same or a similar security incident from reoccurring.

IM-02 Contact points

Clearly appointed points of contact (internal, external, and at Customers) should be in place to ensure a quick and effective response to security incidents. [P1])

The list of contacts should consider the risk of people being unavailable (e.g., to have more than one person and contact method for each escalation point).

The Organisation should have a 24/7 contact number available to respond to critical or significant information security incidents such as zero-day attacks, for example.

A documented process should be in place to notify customers when a security incident occurs. [P1]

The Organization should have a documented process in place that ensures that when the Organization experiences a security incident that could impact the Customer, notifications are sent in a timely manner to Customer's points of contact, with a short description of the incident and its criticality level.

IM-03 Forensic readiness

A documented policy or process should be in place to manage the preservation of evidence relating to security incidents. [P2]

Documentation should be in place to preserve evidence for when disciplinary or legal proceedings are required. This includes the collection, retention and presentation of such evidence.

PS. Physical security

PS-01 Access control

Physical access controls should be in place to restrict the entry and exit of personnel, equipment and media from areas such as office buildings, data centres or rooms where communication servers are located. [P1]

The Organisation should ensure that any equipment and facilities are secured to prevent loss, damage, theft or compromise of Customer information. This includes:

- access control for entrances into the Organisation's data centre (e.g. security guard, badge reader, electronic lock, court admissible CCTV) with logs recorded, reviewed and retained as necessary;
- physical access restricted to those with a business need and the minimum access necessary to do their job;
- control of delivery and loading areas and other points of access where unauthorised persons could enter the premises;
- emergency exit doors should be alarmed, monitored and tested in line with appropriate regional, national and international standards;
- power supplies and fire safety mechanisms undergo regular maintenance checks and comply with Health and Safety regulations; and
- intruder detection systems should be installed, monitored and tested in line with appropriate regional, national and international standards.

PS-02 Environmental threats

Physical protection should be in place to reduce the risk from environmental threats and hazards as well as deliberate attack. [P2]

Environmental threats should be considered, and the risk assessed, especially when delivering a Service. This includes threats such as flood, fire, earthquake, civil unrest and other forms of natural or man-made disaster. Specialist advice may be needed to ensure that there is adequate protection in place.

CS. Cloud Security

CS-01 Cloud-based service adoption procedure

Vendors should provide all information needed by Customer to follow the cloud adoption procedure defined in EBU R 146. [P2]

Recommendation R 146 provides a procedure for the acceptance of cloud-based services by media companies. The Vendor should cooperate and provide all information needed by the media company to follow the procedure, including service functionalities, processes, systems and data, data classification, possible usage limitations according to local or European laws, technical and organizational requirements to operate the service etc.

CS-02 Segregation of Customer data

Appropriate segregation of Customer data should be in place. Customer data should be stored or processed in a multi-tenanted environment. [P1]

If Customer data is hosted on cloud platforms where there are multiple tenants, there should be segregation between Customers so that each Customer's data are kept confidential and are not disclosed to the other Customers and that an incident affecting one Customer does not have an adverse impact on other Customers or their information.

CS-03 Segregation of Customer platforms/infrastructure

Adequate segregation should exist between Customer platforms and infrastructure to allow updates or changes to be applied independently, where required. [P1]

As in section CS-02, there should be segregation between Customers to ensure that if an update or change needs to be applied independently to one Customer, there is no adverse impact to other Customers.

BC. Business Continuity

BC-01 Business continuity planning

A business continuity and/or disaster recovery plan should be in place that is tested and reviewed at regular intervals. [P2]

The Organisation should have a business continuity or disaster recovery plan in place that includes the continuation of security of Customer information in the event of an adverse situation.

As a minimum, the plan should:

- set out how business operations will be restored following an interruption to or failure of business processes within an agreed time period (agreed with the Customer);
- set out how information security will be maintained;
- include arrangements to inform and engage the appropriate Customer personnel in its execution;
- be tested at regular intervals;
- be regularly reviewed and updated where necessary.

In case the Product is a service provided to the Customer, there should be sufficient redundancy to meet the availability requirements for providing the services to the Customer.

BC-02 Utility Service Outages

Security measures should be in place to protect Customer Information in case of utility service outages (e.g., power failures and network disruptions). [P2]

Security measures should be in place to protect Customer information and could include (but is not limited to):

- backup power generation;
- dual/multiple routing;
- load balancing and redundancy;
- bandwidth capacity monitoring and alerting; and

regular testing.

SC. Supply Chain Management

SC-01 Supply chain security control assessment

The Vendor should apply the same level of security control assessment procedure to its own suppliers and subcontractors. [P1]

The Vendor should require its own potential subcontractors, Suppliers and Vendors of main subsystems, software and services that are embedded in their Products to declare their ability to comply with security controls assertation and guidance with the same level of details provided in this Recommendation. Vendors should communicate the results to their Customers.

CM. Change management

CM-01 Change management

Changes that affect the security of the Product or service should be controlled and authorised through a formal, documented process. [P3]

Changes that affect the security of the Product or service should be controlled, documented, and authorised through a formal process. Any such change must be reviewed and tested to ensure that there is no adverse impact on the Product provided to the Customer or to the security of Customer information.

Annex B: Media Appliance Security Requirement

[Information to assist with completion of Worksheet B of the Spreadsheet]

DO. Documentation

DO-01 Password change

There should be explicit instructions to change default passwords, especially in internet facing systems. [P1]

Default passwords are a well-known vulnerability. The documentation issued with the Product should have explicit instructions to change default passwords.

DO-02 Security functionality

Product documentation should include a complete description of security functionality. [P2]

Documentation provided should include details of all the security functionality provided with the Product. This should cover all the requirements in Annex B of this Recommendation as a minimum.

DO-03 Networking

Product documentation should include a complete description of interfaces, access points, network communication and features. [P1]

In detail, the Vendor should provide:

- which Layer 3 capabilities are used;
- which ports are used by the application/system;
- which IP ports are open (not used, but could potentially be used for application attack); and
- which IP ports are disabled as part of the standard application configuration.

DO-04 Integration

Product documentation should include information on how to integrate the Product in a security framework (e.g., different network zones, central authentication service, workflows, interfaces, only necessary TCP/UDP ports are open). [P2]

Clear documentation should be provided that includes detail on how to integrate the Product in various security scenarios.

DO-05 Hardening

The Product should include recommendations on hardening or best practice configuration, including the default state of the Product. Only the minimum required services should be active. [P1]

Where available, industry best practice should be followed for system hardening e.g. CIS Benchmarks or SANS Institute.

Only the minimum required services should be running.

DO-06 Patch management process

Product documentation should include a description of the patch and release management process (especially regarding security updates). [P1]

The patch management and release management documents for the Product should be produced in line with section OS-O3. Product lifecycle.

AA. Authentication & Authorisation

AA-01 Central authentication

The Product should support central authentication services that are most used in the industry. [P2]

The Product should support central authentication services. The following is a list of those that are most used in the industry:

- Active Directory: Kerberos based authentication
- LDAP over SSL: LDAPS
- Identity Provider:
  - SAML IdP: Simple Authentication Mark-up Language
  - OpenID IdP: Identity layer on top of the OAuth protocol
- RADIUS
- TACACS+

AA-02 Session timeout

The Product should support the timeout of sessions. [P2]

Session timeouts should be set with a balance of security and usability. The window of opportunity for an attacker needs to be limited, but a user should be able to comfortably complete operations within the Product without the session timing out too often.

AA-03 Role based access control (RBAC)

The Product should support RBAC. [P2]

Role based access restricts access based on a user's role within an Organisation.

The access to the Product should only be granted for particular capabilities, roles, or users and is not available to anyone. The Product should deny access by default when delivered.

AA-04 Personalised accounts

The Product should support the authentication of individual users. [P2]

Every user should log into the system with a unique personal account to ensure that the individual activity of each person using the account can be identified and audited, and that individual accountability is maintained.

AA-05 Default passwords

The Product should require user to change default passwords for built-in accounts. [P1]

It should be mandatory to change default passwords. As factory or default passwords are often well know and publicly documented, they could be a source of unauthorised access, especially for equipment that is exposed to the internet.

The Product should not have global hidden accounts with the same password or access key for all Product units and Customers. [P1]

Products often embed "hidden" accounts, used by Vendors to perform maintenance tasks (which means that these accounts have high privileges.

AA-06 Password policy

The Product should support a strong password policy implementation. [P1]

To implement strong passwords, the password policy should include as a minimum:

- Minimum password length of 10 characters (longer for administrative accounts, 15 characters are recommended).
- Upper/lowercase characters.
- Numbers.
- Special characters and extended special characters.

AA-07 Authentication

The Product should support enhanced authentication mechanisms such as multi-factor authentication (MFA), in internet-facing interfaces [P1]

Strong authentication mechanisms provide additional layers of security to the traditional authentication scheme. The strong authentication method relies on implementing more than one of the following authentication factors (Multi-Factor Authentication – MFA):

1. Something you know
2. Something you have
3. Something you are

For example, using an authenticator App on a trusted device, a physical security token or a one-time password/code that is regularly refreshed or with a short expiry.

The Product should support enhanced authentication mechanisms (second factor of authentication (2FA) using Security Assertion Mark-up Language V2 (SAML2)) in internet-facing interfaces. This

method can be combined with SSO, allowing users to authenticate only once, and not for each application they access.

AA-08 Authentication, Authorisation and Accounting (AAA) logging

The Product should generate logs for authentication events, authorisation events and user activities as they occur. [P1]

The Product should generate security event logs that record details of:

- **Authentication**: details of any logins to the system and whether they were successes or failures.
- **Authorisation**: details of user attempts to access specific system functions (especially sensitive administrative functions) and whether these were permitted or denied.
- **Accounting**: details of activities / actions undertaken by users on the system.

See also: BA-01 for recommendations on how to manage the logs generated.

EN. Encryption

EN-01 Password storage and transfer

Passwords should neither be stored in the Product nor transferred in plain text or in any reversible format. Onscreen password masking should be implemented. [P1]

The Product should implement onscreen password masking i.e., when typing in a password, the system displays a row of asterisks rather than an actual password. This ensures that the entry of user passwords cannot be observed by another user.

EN-02 Data at rest

The Product should support state-of-the-art encryption technologies following industry best practice recommendations and latest standards. [P2]

Data at rest should be encrypted using state-of-the-art encryption, following common standards such as NIST FIPS 140-3, BSI TR-02102-1 etc. It should be documented which standards the Product uses.

EN-03 Data in transit

The Product should support authenticated and encrypted network protocols. [P1]

Communications should be authenticated and encrypted when transmitted across networks so as to protect against tampering and eavesdropping of network traffic by unauthorized users, following common standards such as BSI TR-02102 series or NIST SP 800-52 Rev.2 etc. It should be documented which standards the Product uses.

- The following protocols should be used:
  - HTTPS

  - SFTP
  - FTPS
  - SCP
  - SSHv2
  - SNMPv3
- The following protocols should be avoided:
  - HTTP
  - FTP
  - TELNET
  - SNMPv1 - SNMPv2
  - SSHv1
  - VNC

EN-04 Certificates Management

Certificates should be securely managed, and regularly renewed. [P2])

Certificates are necessary to authenticate people, devices and services and to secure the transfer of information. Certificate management should follow common standards. The standard that the Product uses should be documented.

EN-05 Cryptographic keys Management

Cryptographic keys should be securely managed. [P1]

Every encryption-based system has a default master key that encrypts all the private keys and passwords in the configuration to secure them. It is recommended to:

- Configure a new master key instead of using the default.
- Change it periodically (the time-period depends on factors such as the criticality/sensitivity of the data being protected).
- Store it in a safe location.

Information on how to configure and potentially reset the master key might also need to be provided by the Vendor.

BA. Base configuration

BA-01 Log management

The Product should generate security event and error logs. [P1]

The Product should, as a minimum, generate the following types of log:

- **Security events**: the system should log AAA data in accordance with AA-08.
- **Errors**: the system should generate error logs when something has gone wrong.

The Product should provide capabilities for securely delivering logs in sync to a centralised log management platform. [P1]

The Product should support regular time synchronisation (e.g., using NTP) with the agreed common reference time-source used by the Organisation deploying it. The investigation of issues is challenging if systems on a network do not use the same time-source.

The Product should support logging through mechanisms that provide assurance that the centralised logging system unequivocally received the data (e.g., TCP preferred over UDP).

The Product should support encryption in transit of log data between the Product and the centralised log management platform.

The product should use documented, standardized and structured formats that can be easily processed by common industry log servers including SIEM solutions.

BA-02 Portable media control

The Product should support disabling or controlling the interfaces and access rights to portable media. [P2]

Portable media (e.g., USB devices) are a frequent route for the introduction of malware, both accidental and deliberate. The Product should support disabling or controlling the interfaces and access rights to this kind of device. The Vendor should explicitly state:

- what interfaces are available;
- the default access rights of the interfaces, and the default operating state (e.g., interfaces activated by default or disabled by default);
- the method needed to enable these interfaces if required.

BA-03 Unnecessary protocol deactivation and OS hardening

Unnecessary protocols should be disabled. [P1]

By default, products should only have needed protocols enabled. Following OS hardening best practices that should be described in the Product documentation (DO-05), it should be possible to disable any protocol/feature that is not needed by the Product.

BA-04 Effective antivirus/malware protection

It should be possible to protect the Product effectively against virus/malware and server-side and client-side exploits. [P1]

The Product should support effective protection against Virus/Malware and server-side and client-side exploits. The Vendor should provide the following detailed information regarding installation and use:

- List of AV solutions that have been tested on the system.
- Installation/update/roll-back methods.

For Systems that cannot meet this requirement, Mandatory Access Control mechanisms like application whitelisting should be put in place.

BA-05 Real-Time Monitoring support

The Product should provide access to data that supports real-time monitoring processes. [P2]

Products should support making system status/health data and performance metrics available by means of an appropriate mechanism (e.g., via SNMPv3) so that they can be monitored using third party monitoring platforms.

BA-06 Backup/restore support

The Product should support backup and restore. [P1]

The Product should support backup and restore, including as a minimum:

- User Data.
- System Data.
- Firmware.
- Configuration.

BA-07 Software/OS decoupling

For media systems running on a general-purpose computer**, the Product should support OS and software decoupling, allowing OS and runtime environments patching. [P1]**

For media systems running on a general-purpose computer, the media vendor's software, system, and services will provide the capability to decouple the operating system from the software itself, thus allowing for the separation of patching of both OS and runtime environments.

NE. Network configuration

NE-01 Network segmentation

The Product should support granular segmentation of networks (MPLS, multi-VLAN, routing). [P1]

The Product should support granular segmentation of networks (MPLS, Multi VLAN, routing). It should also include isolation between management and network traffic, as is done in common network management and monitoring tools.

NE-02 Security of call-home Internet connectivity

If the device requires a default call-home connection, it should be secured by appropriate means. In particular:

The Product should work without needing a constant and direct connection to the internet. [P2]

The Product should support content inspection when connected to the internet. [P1]

This kind of inspection can be implemented through forward and reverse proxies, including authentication mechanisms.

The Product should support jumphost. [P1]

The Product should support maintenance access points in a demilitarized zone (DMZ) so that Vendors or administrators first connect to a DMZ instead of to the appliance itself.

The Product should provide traffic monitoring (inbound/outbound). [P3]

Monitoring or filtering the traffic can be useful to detect abnormal behaviour related to unauthorized activities.

AP. Application security

AP-01 Conformance with industry standard development policies

The media vendor's software development should follow industry-standard development policies (e.g., OWASP Top 10 in its latest version). [P1]

Detail on the controls for application security can be found on the OWASP website https://cheatsheetseries.owasp.org/ .

Annex C: SaaS Security Requirement

[Information to assist with completion of Worksheet C of the Spreadsheet]

DO. Documentation

DO-01 Password change

There MUST be explicit instructions to change default passwords. [P1]

Default passwords are a well-known vulnerability. The documentation issued with the Product should have explicit instructions to change default passwords.

DO-02 Security functionality

Product documentation SHOULD include a complete description of security functionality. [P2]

Documentation provided should include details of all the security functionality provided with the Product. This should cover all the requirements in **Annex B** of this Recommendation as a minimum.

DO-03 Networking

Product documentation MUST include a complete description of interfaces, access points, network communication and features. [P1]

In detail, the Vendor should provide:

- which Layer 3 capabilities are used;
- which ports are used by the application/system;

DO-04 Integration

Product documentation SHOULD include information on how to integrate the Product in a security framework (e.g., different network zones, central authentication service, workflows, interfaces, only necessary TCP/UDP ports are open). [P2]

Clear documentation should be provided that includes detail on how to integrate the Product in various security scenarios.

DO-05 Hardening

The Product MUST include recommendations on hardening or best practice configuration, including the default state of the Product. Only the minimum required services should be active. [P1]

Where available, industry best practice should be followed for system hardening e.g., CIS Benchmarks or SANS Institute.

Only the minimum required services should be running.

AA. Authentication & Authorisation

AA-01: Personalised accounts

The Product MUST support the authentication of individual users. [P1]

Every user should log into the system with a unique personal account to ensure that the individual activity of each person using the account can be identified and audited, and that individual accountability is maintained.

There MUST not be hidden global accounts. Administrators should authenticate as individual users. [P1]

Vendor sometime set hidden global accounts (for example "admin", "root") for system administrators to manage the SaaS Product, including for security auditing or emergency access. They have often high privileges. This put at risk the security of the system. Administrators must authenticate as individual users that can be identified and audited.

AA-02 Multi factor authentication

Multi-factor authentication MUST always be used. [P1]

Strong authentication mechanisms provide additional layers of security to the traditional authentication scheme. The strong authentication method relies on implementing more than one of the following authentication factors (Multi-Factor Authentication – MFA):

1. Something you know
2. Something you have
3. Something you are

For example, using an authenticator App on a trusted device, a physical security token or a one-time password/code that is regularly refreshed or with a short expiry.

The Product should support enhanced authentication mechanisms (second factor of authentication (2FA) using Security Assertion Mark-up Language V2 (SAML2)) in internet-facing interfaces. This method can be combined with SSO, allowing users to authenticate only once, and not for each application they access.

If multi-factor authentication cannot be implemented, the Saas Product may only be accessed from protected data networks (e.g., the broadcaster's data network).

AA-03 Single Sign-on (SSO)

The SaaS Product MUST support Single Sign-On (SSO) through standard federation protocols. [P1]

The SaaS product MUST support SSO through standard federation protocols such as SAMLv2, openid connect, to integrate with corporate identity provider (IdP).

AA-04 Access Control

All users and administrators MUST only have rights required to perform their respective tasks (principle of least privilege). [P1]

The SaaS product should deny access by default, and grant access only when required and with only necessary access rights that each user/process strictly need to perform their tasks.

The Product SHOULD support Role Based Access Control (RBAC). [P2]

Role based access restricts access based on a user's role within an Organisation.

The access to the SaaS Product should only be granted upon request and for particular capabilities, roles, or users and is not available to anyone.

AA-05 Session timeout

The Product SHOULD support the timeout of sessions. [P2]

Session timeouts should be set with a balance of security and usability. The window of opportunity for an attacker needs to be limited, but a user should be able to comfortably use Product without the session timing out too often.

AA-06 User Provisioning

The Product SHOULD support System for Cross Domain Identity Management (SCIM) for user provisioning. [P2]

SCIM is an open standard protocol used to simplify cloud identity and access management across multiple systems, with automatic provisioning and deprovisioning of users.

AA-07 Default authentication information

The Product MUST require the user to change default authentication information. [P1]

It must be mandatory to change default authentication information e.g. default or initial IDs and passwords. As default login and passwords are often well know and publicly documented, they could be a source of unauthorised access.

AA-8 Password policy

The Product MUST support a strong password policy implementation. [P1]

To implement strong passwords, the password policy should include as a minimum:

- Minimum password length of 10 characters (longer for administrative accounts; 15 characters are recommended).
- Upper/lowercase characters.
- Numbers.
- Special characters and extended special characters.

AA-9 Brute Force Protection

The cloud service provider MUST feature effective state-of-the-art brute force protection for all login to the service. [P1]

To avoid Brute force attacks that crack login, passwords or encryption keys a combination of measures should be implemented, including strong password policies, Account lockout after a certain number of failed login attempts, MFA, number of login attempts limited within a time frame.

AA-10 Authentication, Authorisation and Accounting (AAA) logging

The Product MUST generate logs for authentication events, authorisation events and user activities as they occur. [P1]

The Product must generate security event logs that record details of:

- **Authentication**: details of any logins to the SaaS Product and whether they were successes or failures.
- **Authorisation**: details of user attempts to access specific system functions (especially sensitive administrative functions) and whether these were permitted or denied.
- **Accounting**: details of activities / actions undertaken by users on the SaaS Product.

See also: BA-01 for recommendations on how to manage logs generated.

It MUST be possible to restrict access to logging data to a defined group of people. [P1]

EN. Encryption

EN-01 Password storage and transfer

The transfer of passwords MUST be secured with state-of-the-art encryption methods. [P1]

The transfer of passwords must be secured using state--of--the--art encryption, following common standards such as NIST FIPS 140-3, BSI TR-02102 etc. The standards that the Product uses should be documented.

Passwords MUST be stored using current state-of-the-art hashing practices. [P1]

Hashing is a one-way function, making it ideal for password validation. Unlike encryption, which is reversible, hashed passwords cannot be decrypted to obtain the original plaintext. State of the Art hashing is defined in common standards such as NIST FIPS 140-3, BSI TR-02102 etc. The standards that the Product uses should be documented.

EN-02 Data at rest

All data at rest MUST be encrypted by the Vendor using current state-of-the-art encryption procedure. [P1]

Data at rest must be encrypted using state-of-the-art encryption, following common standards such as NIST FIPS 140-3, BSI TR-02102-1 etc. The standards that the Product uses should be documented.

If data at rest is to be decrypted by the Vendor, the purpose of the decryption SHOULD be comprehensibly documented for the Customer. [P2]

Vendor may need to decrypt data at rest for example when checking for malwares. Any decryption of the Customer data should be comprehensibly documented.

EN-03 Data in transit

All data in transit MUST be encrypted using current state-of-the-art encryption procedures. [P1]

Communications must be authenticated and encrypted when transmitted across networks so as to protect against tampering and eavesdropping of network traffic by unauthorized users, following common standards like BSI TR-02102 series or NIST SP 800-52 Rev.2 etc. The standards that the Product uses should be documented.

EN-04 Certificates Management

Certificates managed by Vendor MUST be securely managed, and regularly renewed. [P1])

Certificates are necessary to authenticate people, devices and services and to secure the transfer of information. Certificate management should follow common standards. The standards that the Product uses should be documented.

EN-05 Cryptographic keys Management

Cryptographic keys managed by Vendor MUST be securely managed. [P1]

Every encrypted system has a default master key that encrypts all the private keys and passwords in the configuration to secure them. If Cryptographic keys are managed by the Vendor, the Vendor MUST:

- Configure a new master key instead of using the default.
- Change it periodically (the time period depends on factors such as the criticality/sensitivity of the data being protected).
- Store it in a safe location.

If Cryptographic keys are not managed by the Vendor, Information on how to configure and potentially reset the master key might also need to be provided by the Vendor.

MR. Monitoring and Remediation

MR-01 Security monitoring

The Vendor MUST have security controls in place for operating the Product. [P1]

The Vendor must be able to continuously control security of infrastructure, OS and Application when operating a SaaS Product.

MR-02 Log management

The Product MUST generate security event and error logs. [P1]

The Product should, as a minimum, generate the following types of logs:

- **Security events**: the system should log AAA data in accordance with AA-11.
- **Errors**: the system should generate error logs when something has gone wrong.

The Product MUST provide capabilities for securely delivering logs in sync to a centralised log management platform. [P1]

The Product should support regular time synchronisation (e.g., using NTP) with the agreed common reference time-source used by the Organisation deploying it. The investigation of issues is challenging if systems on a network do not use the same time-source.

The Product should support logging through mechanisms that provide assurance that the centralised logging system unequivocally received the data (e.g., TCP preferred over UDP).

The Product should support encryption in transit of log data between the Product and the centralised log management platform.

The Product should use documented, standardized and structured formats that can be easily processed by common industry log servers including SIEM solutions.

MR-03 Real-Time Monitoring support

The Product SHOULD provide access to data that supports real-time monitoring processes. [P2]

Products should support the making of system status/health data and performance metrics available by means of an appropriate mechanism (e.g., via SNMPv3) so that they can be monitored using third party monitoring platforms.

MR-04 Backup/restore support

The Product MUST support backup and restore. [P1]

The Product must support backup and restore, including as a minimum:

- User Data.
- System Data
- Configuration

MR-05 Patch and Vulnerability Management

Reports of new vulnerabilities in the IT components used MUST be proactively searched for and verified. [P1]

The software and systems used MUST be kept up to date with the latest patches and security-relevant updates MUST be installed immediately. [P1]

New vulnerabilities may be found anytime in software and its sub-components and disclosed. Automatic security scanning tools should be used to detect known vulnerabilities and reports from cybersecurity organisations should be regularly checked. Patches and security updates should be installed immediately to mitigate the risk that attackers exploit these vulnerabilities.

MR-06 Subcontractors

The Vendor MUST provide a list of all subcontractors (sub-service providers) and a clear description of how and to what extent they are involved in the provision of the SaaS Product. [P1]

The Vendor MUST ensure that the security requirements set by the Customer are also met by subcontractors involved in the provision of the SaaS Product. [P1]

The Vendor must continuously monitor the cybersecurity of the subcontractors that are involved in the provision of the SaaS Product.

Any change to contractual agreements with subcontractors (sub-service providers) involved in the provision of the service MUST be communicated to the Customer immediately in writing or by e-mail prior to implementation. [P1]

NI. Network and Infrastructure

NI-01 Data Centre

Physical access and access to data and information MUST follow state-of-the-art security measures. [P1]

State of the Art security measures are listed in section PS. Physical security. In addition to direct access, this also applies to all kind of remote access.

NI-02 Network Infrastructure

State-of-the-art network security measures MUST be established. [P1]

State-of-the-art network security measures include firewalls and network segmentation with different security zones.

NI-03 Infrastructure hardening

The infrastructure used to provision the service MUST be hardened. [P1]

This includes uninstalling unnecessary software packages; deactivating/disabling software, services, accounts and ports that are not required; resetting configurations; enforcing firewall rules.

NI-04 Effective antivirus/malware protection

Adequate and state-of the art protection against virus/malware MUST be established. [P1]

Protecting against viruses and malware is crucial for maintaining the security of network and infrastructure. It includes Signature-based Detection, static and dynamic malware analysis, antivirus Software.

NI-05 DDoS Protection

Measures for the mitigation of Distributed Denial of Service (DDoS) attacks MUST be implemented. [P1]

Measures to mitigate impact of DDoS attacks include monitoring of network traffic, scale up Network Bandwidth, use anti DDoS hardware and Software such as firewalls & intrusion detection/prevention (IDS/IPS).

Data and IPRs

DI-01 Client Separation

Effective client separation MUST be established. [P1]

The Customer's data must be logically separated from other clients' data.

DI-02 Data backup and recovery

The Vendor SHOULD offer state-of-the-art data backup and recovery procedures. [P2]

Data retention periods and recovery times should be implemented according to the Customer's specifications.

DI-03 Exportability / portability

Upon termination of the service agreement, the Customer's data MUST be retrievable and exportable in standard electronic formats. [P1]

Standard electronic formats such as CSV, XML, ZIP archive, should be used for exporting data.

The Vendor MUST provide appropriate interfaces, such as APIs and protocols, for the retrieval of customer data. [P1]

DI-04 Deletion

Upon termination of the service, the Customer's data and information MUST be irreversibly deleted. [P1]

The Customer must not suffer any damage as a result of data that has not been deleted.

The Vendor SHOULD provide to the Customer a proof of deletion. [P2]

Proofs of deletion may be deletion logs or deletion reports that document the data deletion process.

DI-05 Data protection

The Vendor MUST comply with GDPR regulations. [P1]

If personal data is processed (including IP addresses), the Vendor MUST comply with GDPR regulations. As a rule, a Data Processing Agreement (DPA) MUST be concluded with Customer.

DI-06 localisation and place of jurisdiction

If personal data is processed (including the IP address), the Vendor MUST provide comprehensible and transparent information on its jurisdiction and the localisation of data storage, processing and backup. [P1]

The Customer MUST be able to determine the localisation (place/country) of data storage, processing and backup. [P1]

The data and information SHOULD be processed or stored within the European Economic Area (EEA). [P2]

DI-07 Intellectual Property Rights

The Customer MUST retain all copyrights, rights of use or exploitation rights to the data and information stored, processed or backed up as part of the assignment. [P1]

AP. Application security

AP-01 Conformance with industry standard development policies

The media vendor's software development should follow industry-standard development policies (e.g., OWASP Top 10 in its latest version). [P1]

Detail on the controls for application security can be found on the OWASP website https://cheatsheetseries.owasp.org/

Appendix 1: Security Controls Assertation (for information only – use the online spreadsheet)

VENDOR SECURITY (Spreadsheet Worksheet A). To be completed by All			Recommended Priority Level	Priority Level requested by Customer	Do you meet this requirement?	Please provide details to support your response in column A	Reviewer comments
IS. Vendor ISMS – This section sets out your organisation's approach to information security							
IS-01	Cyber security policy	A documented Cyber Security Policy (or set of policies) MUST be in place and approved by senior management	P1				
		Cyber security policies MUST be kept up to date and effectively communicated to all relevant personnel.	P1				
		The Organization SHOULD be certified against recognised security standards and frameworks	P2				
IS-02	Effective cyber security organisation	All cyber security roles and responsibilities SHOULD be assigned and communicated to relevant personnel.	P2				
		There MUST be a named Chief Information Security Officer (CISO) or appointed person who has overall responsibility for cyber security within the organisation.	P1				
		Cyber security awareness training and education SHOULD be provided to all employees (including contractors) as is relevant to their role.	P2				
IS-03	Audit plan	The organisation SHOULD have audit procedures in place that ensure periodic review of the suitability and effective operation of its security controls framework.	P2				

OS. Operational Security							
OS-01	Technical security analysis	Regular technical security analysis such as penetration or vulnerability testing of the product or service MUST be performed.	P1				
OS-02	Vulnerability management	A vulnerability management process MUST be in place to keep track of identified vulnerabilities and patches that may fix them.	P1				
		There SHOULD be a vulnerability disclosure policy or process in place for the responsible reporting of vulnerabilities	P2				
		The Vendor SHOULD implement and follow the Common Vulnerabilities and Exposures (CVE) vulnerability management process for vulnerabilities identified in its own code and systems.	P2				
		The media vendor MUST release information immediately in the event any security vulnerability in its product(s) (own code or third-party code) becomes known	P1				
		A Security Level Agreement MUST be put in place, including maximum time to deliver patches to fix vulnerabilities, depending on their criticality and risk associated to it for the Customer	P1				
OS-03	Product lifecycle	The product lifecycle MUST be clearly defined, and patches and updates MUST be made available throughout that lifecycle, including for all third-party components embedded in Product	P1				
OS-04	Product/software delivery	A secure process SHOULD be in place for the delivery of products, software or services.	P2				
OS-05	Customer maintenance	Maintenance and Remote support to Customer MUST be provided securely	P1				

OS-06	Separation of production and non-production	Production and non-production environments SHOULD be kept separate.	P2				
SD. Secure Development							
SD-01	Development lifecycle	Security SHOULD be designed into and implemented through the whole lifecycle of product development.	P2				
SD-02	Training	Development staff SHOULD be trained in the latest secure coding principles and industry good practice.	P2				
SD-03	Source code	Access to proprietary program source-code SHOULD be restricted and strictly controlled.	P2				
IM. Incident Management							
IM-01	Incident response	A documented incident response and crisis management process/procedure MUST be in place, that is regularly reviewed and kept up to date.	P1				
IM-02	Contact points	Clearly appointed points of contact (internal, external, and at customers) MUST be in place to ensure a quick and effective response to security incidents.	P1				
		A documented process MUST be in place to notify customers when a security incident occurs	P1				
IM-03	Forensic readiness	A documented policy or process SHOULD be in place to manage the preservation of evidence relating to security incidents.	P2				
PS. Physical Security							
PS-01	Access control	Physical access controls MUST be in place to restrict the entry and exit of personnel, equipment and media from areas such as office buildings, data centres or rooms where communication servers are located.	P1				
PS-02	Environmental threats	Physical protection SHOULD be in place to reduce the risk from environmental threats and hazards as well as deliberate attack.	P2				

CS. Cloud Security							
CS-01	Cloud based service adoption procedure	Vendors SHOULD provide all information needed by customer to follow the cloud adoption procedure defined in EBU R 146	P2				
CS-02	Segregation of customer data	Appropriate segregation of customer data MUST be in place. Customer data MUST be stored or processed in a multi-tenanted environment.	P1				
CS-03	Segregation of customer platforms/infrastructure	Adequate segregation MUST exist between customer platforms and infrastructure to allow updates or changes to be applied independently, where required.	P1				
BC. Business Continuity							
BC-01	Business continuity	A business continuity and/or disaster recovery plan SHOULD be in place that is tested and reviewed at regular intervals.	P2				
BC-02	Utility Service outages	Security measures SHOULD be in place to protect Customer information in case of utility service outages (e.g., power failures and network disruptions).	P2				
SC. Supply Chain Management							
SC-01	supply chain security control assessment	The Vendor MUST apply the same level of security control assessment procedure to its own suppliers and subcontractors.	P1				
CM. Change Management							
CM-01	Change management	Changes that affect the security of the product or service SHOULD be controlled and authorised through a formal, documented process.	P3				

PRODUCT SECURITY (Spreadsheet Worksheet B). For Media Appliance Vendors.			Recommended priority level	Priority Level requested by Customer	Do you meet this requirement?	Please provide details to support your response in column A	Reviewer comments
DO. Documentation							
DO-01	Password change	There MUST be explicit instructions to change default passwords, especially in internet facing systems.	P1				
DO-02	Security functionality	Product documentation SHOULD include a complete description of security functionality.	P2				
DO-03	Networking	Product documentation MUST include a complete description of interfaces, access points, network communication and features.	P1				
DO-04	Integration	Product documentation SHOULD include information on how to integrate the Product in a security framework (e.g., different network zones, central authentication service, workflows, interfaces, only necessary TCP/UDP ports are open).	P2				
DO-05	Hardening	The Product MUST include recommendations on hardening or best practice configuration, including the default state of the Product. Only the minimum services required MUST be active.	P1				
DO-06	Patch management process	Product documentation MUST include a description of the patch and release management process (especially regarding security updates).	P1				
AA. Authentication & Authorisation							
AA-01	Central authentication	The Product SHOULD support central authentication services that are most used in the industry.	P2				
AA-02	Session timeout	The Product SHOULD support the timeout of sessions.	P2				
AA-03	Role based access control (RBAC)	The Product SHOULD support RBAC.	P2				
AA-04	Personalised accounts	The Product SHOULD support the authentication of individual users.	P2				

AA-05	Default passwords	The Product MUST require user to change default passwords for built-in accounts	P1				
		The Product MUST NOT have global hidden accounts with the same password or access key for all Product units and customers.	P1				
AA-06	Password policy	The Product MUST support a strong password policy implementation.	P1				
AA-07	Authentication	The Product MUST support enhanced authentication mechanisms such as multi-factor authentication (MFA) in internet-facing interfaces or for internet-facing services.	P1				
AA-08	Authentication, Authorisation and Accounting (AAA) logging	The Product MUST generate logs for authentication events, authorisation events and user activities as they occur	P1				
EN. Encryption							
EN-01	Password storage and transfer	Passwords MUST neither be stored in the Product nor transferred in plain text or in any reversible format. Onscreen password masking MUST be implemented	P1				
EN-02	Data at rest	The Product SHOULD support state-of-the-art encryption technologies following industry best practice recommendations and latest standards.	P2				
EN-03	Data in transit	The Product MUST support authenticated and encrypted network protocols	P1				
EN-04	Certificates management	Certificates SHOULD be securely managed, and regularly renewed.	P2				
EN-05	Cryptographic	Cryptographic keys MUST be securely managed.	P1				

BA. Base configuration							
BA-01	Log management	The Product MUST generate security event and error logs	P1				
		The Product MUST provide capabilities for securely delivering logs in sync to a centralised log management platform	P1				
BA-02	Portable media control	The Product SHOULD support disabling or controlling the interfaces and access rights to portable media.	P2				
BA-03	Unnecessary protocol deactivation and OS hardening	Unnecessary protocols MUST be disabled	P1				
BA-04	Effective antivirus/malware protection	It MUST be possible to protect the Product effectively against virus/malware and server-side and client-side exploits	P1				
BA-05	Real time Monitoring support	The Product SHOULD provide access to data that supports real-time monitoring processes	P2				
BA-06	Backup/restore support	The Product MUST support backup and restore	P1				
BA-07	Software/OS decoupling	For media systems running on a general-purpose computer, the Product MUST support OS and software decoupling, allowing OS and runtime environments patching	P1				

NE. Network configuration							
NE-01	Network segmentation	The Product MUST support granular segmentation of networks (MPLS, multi-VLAN, routing)	P1				
NE-02	Security of call home Internet connectivity	The Product SHOULD work without needing a constant and direct connection to the internet	P2				
		The Product MUST support content inspection when connected to the internet	P1				
		The Product MUST support jumphost	P1				
		The Product SHOULD provide traffic monitoring (inbound/outbound)	P3				
AP. Application security							
AP-01	Conformance with industry standard development policies	The media vendor's software development MUST follow industry-standard development policies (e.g., OWASP Top 10 in its latest version).	P1				

PRODUCT SECURITY (Spreadsheet worksheet C). For SaaS Vendors.			Recommended priority level	Priority Level requested by Customer	Do you meet this requirement?	Please provide details to support your response in column A	Reviewer comments
DO. Documentation							
DO-01	Password change	There MUST be explicit instructions to change default passwords.	P1				
DO-02	Security functionality	Product documentation SHOULD include a complete description of security functionality.	P2				
DO-03	Networking	Product documentation MUST include a complete description of interfaces, access points, network communication and features.	P1				
DO-04	Integration	Product documentation SHOULD include information on how to integrate the Product in a security framework (e.g., different network zones, central authentication service, workflows, interfaces, only necessary TCP/UDP ports are open).	P2				
DO-05	Hardening	The Product MUST include recommendations on hardening or best practice configuration, including the default state of the Product. Only the minimum services required MUST be active.	P1				
AA. Authentication & Authorisation							
AA-01	Personalised accounts	The Product MUST support the authentication of individual users	P1				
		There MUST NOT be hidden global accounts	P1				
AA-02	Multi-factor Authentication	Multi-factor authentication MUST always be used	P1				
AA-03	Single Sign On (SSO)	The Saas Product MUST support Single Sign On through standard federation protocols	P1				
AA-04	Access control	All users and administrators MUST only have rights required to perform their respective tasks (principle of least privilege)	P1				

		The Product SHOULD support Role Based Access Control (RBAC)	P2				
AA-05	Session timeout	The Product SHOULD support the timeout of sessions.	P2				
AA-06	User provisioning	The Product SHOULD support System for Cross Domain Identity Management (SCIM) for user provisioning	P2				
AA-07	Default authentication information	The Product MUST require user to change default authentication information	P1				
AA-08	Password policy	The Product MUST support a strong password policy implementation.	P1				
AA-09	Brute force penetration	The cloud service provider MUST feature effective state-of-the-art brute force protection for all logins to the service	P1				
AA-10	Authentication, Authorisation and Accounting (AAA) logging	The Product MUST generate logs for authentication events, authorisation events and user activities as they occur	P1				
	Restricted access to logging data	It MUST be possible to restrict access to logging data to a defined group of people	P1				
EN. Encryption							
EN-01	Password transfer	The transfer of passwords MUST be secured with state-of-the-art encryption methods	P1				
	Password storage	Passwords MUST be stored using current state-of-the-art hashing practices	P1				
EN-02	Data at rest	All data at rest MUST be encrypted by the Vendor using current state-of-the-art encryption procedures	P1				

	Data at rest	If data at rest is to be decrypted by the Vendor, the purpose of the decryption SHOULD comprehensively be documented for the Customer	P2				
EN-03	Data in transit	All data in transit MUST be encrypted using current state-of-the-art encryption procedures	P1				
EN-04	Certificates management	Certificates managed by Vendor MUST be securely managed, and regularly renewed.	P1				
EN-05	Cryptographic keys management	Cryptographic keys managed by Vendor MUST be securely managed.	P1				
MR. Monitoring and Remediation							
MR-01	Security monitoring	The Vendor MUST have security controls in place for operating the Product	P1				
MR-02	Log management	The Product MUST generate security event and error logs	P1				
		The Product MUST provide capabilities for securely delivering logs in sync to a centralised log management platform	P1				
MR-03	Real time Monitoring support	The Product SHOULD provide access to data that supports real-time monitoring processes	P2				
MR-04	Backup/restore support	The Product MUST support backup and restore	P1				
MR-05	Patch and vulnerability management	Reports of new vulnerabilities in the IT components used MUST be proactively searched for and verified	P1				

		The software and systems used MUST be kept up to date with the latest patches and security-relevant updates MUST be installed immediately	P1				
MR-06	Subcontractors	The Vendor MUST provide a list of all subcontractors (sub-service providers) and a clear description of how and to what extent they are involved in the provision of the service.	P1				
		The Vendor MUST ensure that the security requirements set by the Customer are also met by subcontractors involved in the provision of the SaaS Product.	P1				
		Any change to contractual agreements with subcontractors (sub-service providers) involved in the provision of the service MUST be communicated to the Customer immediately in writing or by e-mail prior to implementation.	P1				
NE. Network and Infrastructure							
NI-01	Data centre	Physical access and access to data and information MUST follow state-of-the-art security measures.	P1				
NI-02	Network Infrastructure	State-of-the-art network security measures MUST be established.	P1				
NI-03	Infrastructure Hardening	The infrastructure used to provision the service MUST be hardened.	P1				
NI-04	Effective antivirus/malware protection	Adequate and state-of the art protection against virus/malware MUST be established.	P1				
NI-05	DDoS Protection	Measures for the mitigation of Distributed Denial of Service (DDoS) attacks MUST be implemented.	P1				
DI. Data and IPRs							
DI-01	Client separation	Effective client separation MUST be established.	P1				

DI-02	Data backup and recovery	The Vendor SHOULD offer state-of-the-art data backup and recovery procedures.	P2				
DI-03	Exportability / portability	Upon termination of the service agreement, the Customer's data MUST be retrievable and exportable in standard electronic formats.	P1				
		The Vendor MUST provide appropriate interfaces, such as APIs and protocols, for the retrieval of customer data.	P1				
DI-04	Deletion	Upon termination of the service, the Customer's data and information MUST be irreversibly deleted.	P1				
		The Vendor SHOULD provide to the Customer a proof of deletion.	P2				
DI-05	Data protection	The Vendor MUST comply with GDPR regulations.	P1				
DI-06	Localisation and place of jurisdiction	If personal data is processed (including the IP address), the Vendor MUST provide comprehensible and transparent information on its jurisdiction and the localisation of data storage, processing and backup.	P1				
		The Customer MUST be able to determine the localisation (place/country) of data storage, processing and backup.	P1				
		The data and information SHOULD be processed or stored within the European Economic Area (EEA).	P2				
DI-07	Intellectual property rights	The Customer MUST retain all copyrights, rights of use or exploitation rights to the data and information stored, processed or backed up as part of the assignment.	P1				
AP. Application security							
AP-01	Conformance with industry standard development policies	The media Vendor's software development MUST follow industry-standard development policies (e.g., OWASP Top 10 in its latest version).	P1				