# BoostAeroSpace Security Policy V1.3

*Effective Date: 27/09/2016*

Index:

## Signature Page

Validation of this document, recorded by BoostAeroSpace Chief Information Security Officer Romain BOTTAN, as been done by the following SMA members:

Airbus Group SMA representative: Gilbert BOURRY

Airbus SMA representatives: Gil MULIN

Dassault Aviation SMA representative: Christophe FLOCH

Safran SMA representative: Frederic GOURJAULT

Thales SMA representative: Bernard DENIS

_____ 27/09/2016

BoostAeroSpace Security Management Authority Date

## Reading instructions

In order to simplify the BoostAeroSpace (BAS) Security Policy reading, each paragraph has been associated with a sign-mark indicating the subject and if relevant the third parties involved in each rule execution. Please refer to the list bellow while reading this policy:

| | |
|---|---|
| (President) | BAS President, representatives |
| (SMA) | BAS Security Management Authority (BAS SMA), representatives |
| (CISO) | BAS Chief Information Security Officer (BAS CISO) |
| (UsMgr) | BAS Users Manager |
| (User) | BAS User |
| (SP) | BAS Service provider |

## Glossary:

| | |
|---|---|
| Hub BoostAeroSpace | Applications and services collaborative platform implemented by the service providers validated by the Security Management Authority of BoostAeroSpace. |
| BAS | Acronym for **B**oost**A**ero**S**pace. |
| Trust Security Baseline | BoostAeroSpace trust & security fundamentals document (refer to annex for details). |
| CEO | Acronym for **C**hief **E**xecutive **O**fficer. |
| SMA Charter | Document outlining the basic principles of the BoostAeroSpace Security Management Authority organization and management. |
| Founding members of the Hub | Companies participating financially and functionally to the creation of the HUB BoostAeroSpace. |
| Hub Partners | Member companies of the HUB BoostAeroSpace. For its creation, only members of the HUB founders are registered as partners of the HUB. |
| CISO | Chief Information Security Officer senior-level executive responsible for establishing and maintaining the enterprise security vision, strategy and program to ensure information assets are adequately protected. |
| Circle of Trust | All customers, service providers and partners of the HUB. |
| SOP ([fr]:PES) | Safe Operating Procedures (in French *"Procedure d'Exploitation de Securité").* Safe operating procedures are written guidelines for procedures and tasks involving recognized hazards. |
| Hub Identity Repository | List of BAS services users identifiers associated to companies. |
| Service Provider | Any person or entity or public entity or group of such persons and / or agencies that offer, respectively, the execution of works and / or work, BoostAeroSpace related products or services on the market. |
| External network | Computer network outside of the partner or service provider network responsibility. |
| SMA | Security Management Authority: BoostAeroSpace security entity making security recommendations in charge of the validations of the BoostAeroSpace hub security. |
| Due care | Responsibility that manager and their organizations have a duty to provide for information security to ensure that the type of control, the cost of control, and the deployment of control are appropriate for the system being managed. |
| Due diligence | Number of concepts involving either an investigation of a business or person prior to signing a contract, or an act with a certain standard of care. It can be a legal obligation, but the term will more commonly apply to voluntary investigations. A common example of due diligence in various industries is the process through which a potential acquirer evaluates a target company or its assets for acquisition. |

# 1. Security Policy Baseline

*Objective: To provide the information security guidance and support from management, according to business requirements, laws and related regulations.*

The Hub Security Policy defines the principles and rules in order to **protect the assets of each BoostAeroSpace client, and his own company on due care principle.**

## 1.1. Information security policy document

*(User)*

Security Policy must be known to all parties involved in the Hub. It will be **notably attached to BoostAeroSpace employment contracts** and to service contracts binding the **hub to its users**.

Documents relating to the BoostAeroSpace security policy are organized in a cascade including those provided in the appendix (see appendix with version):

- Trust_Security_Baseline [RD02]
- BAS_Security_Policy (this document) [RD03]
- Boost_Bridge_Certificate_Policy [RD04]
- BoostAeroSpace_SMA_Code_Of_Etics [RD05]

## 1.2. Review of the information security policy

*(SMA, CISO, President)*

The security policy of the Hub must be reviewed every 2 years or at the request of one BAS partner or BAS CEO (e.g. in case of arrival of a new partner), in regards of the defined update governance arrangements.

## 1.3. Trust Security baseline of the BoostAeroSpace HUB

The basic principles mentioned below are written in reference with document "Trust_Security_Baseline [RD02].

### 1.3.1. Security Management Authority

*SMA to User, SP*

The SMA is the entity of specifications, control and validation of the security of the hub. It also qualify the security equipments (encryption, PKI, firewalls ...). Its composition, operating methods and roles are defined in the SMA charter [RD05].

The SMA defines and updates the security policy and may request to audit:

a) the compliance with security policy for the implementation of the HUB;
b) the compliance with security policy for HUB users and services providers.

### 1.3.2. Fundamentals

*(User, SP)*

All data hosted in the Hub reach the maximum level of "confidential industrie."

This excludes in particular any data classified “Secret Défense” or relative with restrictive local regulations.

*(SP) to (SMA)*

Data hosted by BoostAeroSpace[1] are physically hosted in BoostAeroSpace company selected premises under agreement of the SMA. **Any modification in the data hosting location including backups must be validated by the SMA.**

*(SP)*

Any modification of the host company will imply that the host complies with the relevant PSSI version at the date of change.

*(User, UsMgr, SP)*

### 1.4. Information security policy compliance

Each signatory of this security policy must produce the documents necessary to proof that he comply with it and should be audited for compliance by the SMA.

## 2. Organization of HUB Information Security

### 2.1. Internal organization

*(SMA, President)*

- SMA

  The SMA is the authority that takes the security decisions for the Hub, in conjunction with both the security function of the President and the Board of Directors of BoostAeroSpace.

  SMA is composed of the CISO of all founding members. Its structure, its internal way of functioning and its interactions with other organs of the hub and external agencies are detailed in the SMA charter [RD05].

*(SP) to (CISO) then (CISO) to (SMA)*

- The BAS CISO

  The BAS organization chart includes a CISO who is part of BoostAeroSpace operational functions.

  Under the authority of the SMA, his mission is to implement and enforce by BoostAeroSpace & Services Providers the security policy and ensure operational security reporting to the SMA.

### 2.2. External Parties

*(SMA)*

- Agreements and commitments

  Any application to the hub (customers, partners, service providers) requires:

  - A pre-approval process from the SMA, including a security compliance audit;

*(UsMgr)*

  - A contractual **commitment of the third party to comply with and enforce the security policy of the HUB to his personal.**

[1] The owners of these data are the partners and / or customers

*(SMA)*

Contractual agreements between partner organizations, suppliers, hub customers and third parties in the BoostAeroSpace scope must cover all security requirements validated by the SMA. These **security requirements** belong to access, processing, communication or information management, and ways of processing information.

*(SP, SMA)*

- Service providers obligations and responsibilities

The service providers shall **provide to companies systems & network the best security they can offer to HUB to protect companies Data they handle and host as well as ensuring the best data access segregation between companies and access methodologies**, in accordance with the classification of the data, the BoostAeroSpace security policy and the guidelines defined by the SMA.

*(SP)*

Service providers need in particular to **monitor** following this Security Policy, ensure the **security reporting** to the SMA and **provide security reports and alerts on expected time**.

Service providers must submit, to the approval of the SMA, their business operations plan including operating procedures for safety (PES) in accordance with this security policy.

The rules of these principles are detailed in their respective chapters later in this document.

# 3. Asset Management

## 3.1. Responsibilities for assets

*(President) to (CISO) then (CISO) to (SMA)*

*Objective: Establish and maintain appropriate protection of partners & BoostAeroSpace company assets.*

A strict assets inventory of the BoostAeroSpace Company must be established and maintained. The ownership of all information and its associated means of processing must be clearly established.

The document "rules of usage and operation of assets" [RD01] describing the rules of usage and operation of Hub assets is **maintained by the BoostAeroSpace company**, **validated by the CISO** of BoostAeroSpace and **approved by the SMA**.

## 3.2. Information classification

*Objective: Ensure that information receive appropriate level of protection.*

*(User)*

- Guidelines

The sensitivity of the information must be characterized in terms of heritage value, legal requirement, and criticality. It belongs to the **owners of each piece of information to determine its level of sensitivity and the right to know (access rights and restrictions of diffusion), in compliance with applicable laws and regulations.**

| | |
|---|---|
| *(SMA)* | The document "information classification" [RD06] written by the SMA defines the possible and excluded levels of classifications. |
| *(User, UsMgr)* | - Marking and manipulation of information<br>The technical infrastructure of the Hub will host only information classified "Confidential Industry" as a maximum, that the Partners agree to share with one or more third parties (partner / supplier) strictly identified. |
| *(SP) to (SMA)* | **All data hosted on the hub is considered according to its classification level, by default "BoostAeroSpace Industry Confidential",** therefore all the technical (infrastructure, IS architectures, storage, backups, operations and administration) must meet the rules defined for this level of sensitivity, by BoostAeroSpace and validated by the SMA. |
| *(User)* | All media must be marked "**BoostAeroSpace Industry Confidential**" when generated, exchanged and stored in the infrastructure of the Hub.<br>The rules for handling, transmitting of information and access controls are addressed in their respective chapters. |

# 4. Human Resources

## 4.1. Hub & services providers human Resources

### 4.1.1. Prior to Hub hiring

*(President, SP)*

The roles and responsibilities of employees, personal of service providers must be formalized and contracted.

Controls of identity details concerning all Personal must:

- be conducted in accordance with laws, regulations and ethics
- be consistent with the function associated in the HUB and classification of confidential industry data manipulated.
- be conform with the list of identifiers of HUB users [RD07].

*(SP)*

As part of their contractual obligations, employees and service provider staff must accept and sign the terms and conditions of their employment contract, which must include their responsibilities and those of their organization for the information security hosted by HUB.

### 4.1.2. During the term of the letter of employment

*(President, SP)*

Each board of directors must require from its employees to apply the security rules and procedures established for the Hub.

All employees of the Hub must receive technical and security appropriated training and updates in line with their functions inside the hub.

There must be a formal disciplinary process for personal responsible of a security breach.

*(President, SP)*

#### 4.1.3. Termination or change of employment

The responsibilities of operations caused by a cessation or change of function must be strictly defined and assigned.

At the end of their work, their contract or their mission, all personals must give back all assets of the organization in their possession.

Access rights to information and information processing infrastructure of all staff who end a mission or a contract must be taken away, or must be modified in case of a change of function.

*(User)*

### 4.2. Hub users

Hub users must sign their acceptance of the terms and conditions of use of the Hub [RD09].

These conditions must cover their responsibilities in terms of:

- The respect of the "acceptable use policy for users & administrators of BoostAeroSpace Hub" [RD09] and this security policy that list the rights and obligations of BoostAeroSpace and services providers.

## 5. Physical and environmental protection

### 5.1. Secure areas

*(User, UsMgr, SP) to (SMA)*

*Objective: Prevent unauthorized physical access, damage or intrusion on **the premises or on partners information.***

The measures adopted to achieve this objective will be evaluated by the SMA or by entity mandated by the SMA for monitoring compliance with the principles of the security policy, particularly on **the basis of best practices as described in ISO 27002.**

Areas of storage of media containing data from backups are subject to the same requirements that are defined for areas containing the systems and data.

*(SP)*

#### 5.1.1. Physical Security Perimeter

All the technical infrastructure of the Hub is in a secured physical environment.

*(User, UsMgr, SP)*

Areas containing information and information means of processing must be protected by security perimeters (**barriers such as walls, doors with access control cards, or offices with reception staff**).

*(SP)*

#### 5.1.2. Physical Access Control

Secure areas must be protected by controls at the entrance to ensure that only authorized personnel are allowed to enter.

Security devices in the zones must also allow limiting access to the HUB components strictly to component's access authorized personnel.

*(UsMgr, SP)*

Access control and traceability of access must be insured individually.

| | |
|---|---|
| *(SP)* | Service providers will include in their operating procedures for safety the description of security measures relating to:<br>a) Offices, rooms and equipment security;<br>b) Work in secure areas;<br>c) Public access areas. |
| *(User, UsMgr)* | **5.1.3. Environmental Protection**<br>Sites and local hosting HUB data must:<br>Have **safeguards systems against environmental threats in accommodation with the hosting context.** |
| *(SP)* | Ensure the **security of functioning of the HUB services and hosted data non-modification**. |
| *(SP) to (SMA)* | These systems will be **submitted to the approval of the SMA**. |
| *(SP)* | **5.2. Equipment security**<br>*Objective: To prevent loss, damage, theft or compromise of assets and the disruption company activities.*<br>Service providers will include in their operating procedures for safety chapters describing the safeguards systems in place, including:<br>a) Equipements location and protection measures;<br>b) security measures for the General Services;<br>c) wiring security;<br>d) security measures applicable to the maintenance of equipment;<br>e) Security of equipment out of the Hub premises;<br>f) disposal or recycling of equipment;<br>g) procedures for the disposal of an asset outside of its premises. |
| *(SP) to (SMA)* | These procedures will be evaluated (& validated) by the SMA, for compliance control with the principles of the Security policy, on the basis of good practices described in ISO 27002 |
| *(SMA)* | **6. Operations & telecommunications management**<br>The measures adopted to achieve this objective will be evaluated by the SMA or an entity mandated by the SMA, for compliance control with the principles of the PSSI, particularly on the basis of best practices described in ISO 27002 |

## 6.1. Operational procedures and responsibilities

*Objective: Ensure the correct and secure operation of information processing infrastructure.*

*(SP) to (SMA)*

Service providers will communicate to the SMA the details of their operating procedures on those security arrangements:

a) compatibility between the human resource allocation and BoostAeroSpace service constraints & accreditations;
b) the impact measurement and non-security regression in the context of changes management.
c) separation of operational tasks;
d) system management function with dedicated system management console networks;
e) separation of development, integration and operational environments;
f) the absence of Internet connection possibility for computers and privilege accounts used in the scope of the HUB system management.

These dispositions will be submitted to approval to the SMA with the communication of service providers' procedures.

## 6.2. Third party service delivery management

*Objective: Implement and maintain adequate information and service security level complying with services offering agreements linked to resources management such as system administration, network monitoring and* preventive maintenance*.*

*(SP) to (SMA)*

Unless otherwise accompanied by a waiver form granted by the SMA, service offer will be performed on a dedicated environment, without continuous access to the production platform. If needed, depending on operational constraints, a temporarily access may be given in consultation on the production platform, only by the SMA or any mandated, and under the conditions validated by the SMA.

*(SP)*

Whatever the location of computer resources, service providers committed to implement the means and procedures to effectively control access to these resources (limitation staff roles and privileges to the minimum necessary to achieve their mission).

*(SP)*

These methods and procedures must be established to ensure actual and unambiguous individual traceability of physical person who accessed these resources:

Accesses to computing resources are nominally assigned to each physical person concerned.

*(SP)*

Immediate deactivation of an account must be done in the following cases:

End of mission of provider staff for any reason including compromising or suspected compromising of his access account.

| | |
|---|---|
| *(SP) to (SMA)* | For all operating / administration offer, services provider must implement strong authentication methods in accordance with the requirements set by the SMA:<br>a) the service provider must establish and maintain with the SMA an escrow of all "administrators" accounts of which he manages;<br>b) if the service provider request for the execution of the service, experts intervention that could respond to emergencies, service provider will use, if any, accounts following an emergency access procedure including an explicit agreement of a representative of the SMA;<br>c) the systems management platform must be on an isolated network, protected by a firewall against external intrusions and contain no links to third party networks and / or Internet network without explicit permission from the SMA; |
| *(SP)* | d) any remote operation on BAS platform device (network device, application server, etc.) must comply with security measures described in section 7.8, "Remote administration".<br>Service delivery management must comply with **due diligence** principle. |
| *(UsGm, SP, President)* | **6.3. Protection and integrity of information**<br>*Objective: Ensure the integrity of the means of treatment, accommodation and data hosted in the HUB.*<br>Each partner, customer, service provider, agrees to implement mechanisms ensuring the protection and integrity of information hosted and processed by the hub, including:<br>a) the adapted protection devices (anti-intrusion devices, DMZ, rebuilding neutral zone,...) must be under constant monitoring;<br>b) measures of detection, prevention and recovery to protect against malicious code;<br>c) appropriated procedures of users awareness for all services of the Hub. |
| *(Us, UsGm, SP)* | Any changes of the HUB content go through a qualification environment before deployment<br>Antiviral policy must take into account an antiviral prevention, anti-malware and intrusion detection on all clients' workstations and all servers. |
| *(User, UsGm, SP) to (SMA)* | A patch management policy validated by the SMA must be applied on all workstations and all servers. This policy must include at minimum the application of security patches in a timely fashion consistent with the criticality of the vulnerabilities covered with one hand and on the other, the regular updates of software releases (to ensure that they are continuously supported by the publisher).<br>Each partner, customer and service provider also undertakes to alert the operational hub services in accordance with paragraph dealing with the security incident management of this document **in case of virus attacks and contribute to viral Hub crisis management.** |
| *(SMA)* | These measures will be evaluated and approved by the SMA, for compliance monitoring with the principles of the BoostAeroSpace Security policy. |

## 6.4. Backup and Restore

*Objective: Maintain the integrity and availability of information and means of information processing*

*(SP)*

The measures must be implemented to ensure continuity of service and availability of data in accordance with:

a) the expected systems and data availability, data integrity service;
b) systems and data availability, data integrity security standards set by the SMA;
c) rules and principles of backups and restorations written in the BoostAeroSpace backups policy [RD15]

*(SP) to (SMA)*

The media routing between operations sites and storage site must be secured following measures approved by the SMA.

*(SP) to (SMA)*

At minimum must be implemented those measures:

a) Architecture with a sufficient level of redundancy;
b) Strategy of backup and restore including the launch, processing monitoring and recovery testing (business continuity);
c) Creation and provision of backups recovery tests execution reports and procedures and dashboards;
d) Storage media backups in a secure location, with frequency agreed by the SMA, to guarantee the recovery capability in case of an incident;
e) Computer media containing data BoostAeroSpace dedicated and labeled;

These measures must be evaluated (and approved) by the SMA, for purposes of monitoring compliance with the principles outlined in this document on this subject.

## 6.5. Network Security

*Objective: To ensure protection of information on networks and protect the infrastructure upon which it rely.*

The technical infrastructure supporting the systems are installed on Hub servers and a dedicated network (called Private Network) for this purpose and physically separated from any other system.

Network infrastructure and communications of the hub must guarantee the security of information of the partner's heritage.

*(SP)*

Their implementation and any changes must be validated prior to their implementation by the SMA.

Infrastructure and communication networks must meet the following requirements including:

a) DMZ and private network of the Hub are not accessible or visible from external networks;
b) inflows and outflows must be analyzed and filtered by equipment DMZ;
c) anyone accessing the services available in the DMZ must be previously identified and authenticated,
d) The level of security required for the authentication means is defined in regards of the service accessed (system and data) and the origin of the connection (workstation / network).

| | |
|---|---|
| | The provision of data from the hub private network is provided by proxy relay systems or replication in DMZ by the help of secured devices.<br><br>All flows of information transmitted via networks not recognized as "**trusted networks**" by the SMA must be encrypted. |
| *(SP) to (SMA)* | The means of encryption must be implemented in accordance with the laws and regulations in regards of context, based on European technology and be subject to prior validation of the SMA<br><br>The configuration and administration of peripheral equipment and security devices are under controlled and monitored using procedures validated by the SMA. Any change in configuration of such equipment must be previously approved by the SMA.<br><br>Configuration and administration process of network and security equipment must be defined, implemented and monitored to prevent any attack or intrusion from the networks.<br><br>The log measures must enable:<br>a) to ensure traceability of all events;<br>b) to ensure non-alteration of logs for 1 year;<br>c) to centralize logs from the different devices for reporting and investigative actions.<br><br>These measures are validated by the SMA and audited by the SMA. |

## 6.6. Media Handling

*Objective: To prevent the disclosure, alteration, unauthorized removal or destruction of assets and interruption of services.*

| | |
|---|---|
| *(SP)* | These rules apply to all services of BoostAeroSpace.<br><br>Service providers and BoostAeroSpace hosts must include in their operating procedures and formally the following security measures:<br>a) The relevant data storage media security rules (storage, transport);<br>b) The storage of BoostAeroSpace information storage media must be in a controlled area, restricted to a level equivalent to the system hosting the BoostAeroSpace data. |
| *(SP)* | Transport of storage media must ensure:<br><br>a) the storage media protection against unauthorized access, misuse, prevention of risk of damage during transportation;<br>b) traceability up to date storage media location modification;<br>c) Procedures and measures for controlled disposal of information storage media, with systematic destruction of the storage media in case of definitive disposal (using measures approved by the SMA)<br>d) Reuse of storage media, with strong pre-clearing measures validated by the SMA, and following a process of erasing written by the host company.<br>e) Labeling media in accordance with the classification rules of § 3.2 |
| *(SP) to (SMA)* | These procedures must be evaluated by the SMA for conformity compliance with the principles of the security policy, particularly on the basis of best practices described in ISO 27002. |

### 6.7. Electronic commerce services

*Objective: To ensure the security of electronic commerce services and their safe use*

Not applicable in the current scope of the HUB, this chapter will be reviewed in a future version.

The information of e-commerce[2], crossing the public network must be protected against any fraudulent activity, contract litigation, disclosure and unauthorized modification.

### 6.8. Monitoring, alerting and reporting

*Objective: To detect and allow managing of incidents and malfunctions*

*(SP)*

Service providers of the Hub must define and implement procedures and devices covering the following points:

a) Operation on audit logs (record user activities, exceptions and events related to security that must be produced and kept for a period previously established to facilitate further investigation and monitoring of access control);
b) Log infrastructure and information protection against alteration and unauthorized access including to the staff responsible for the operation and administration of HUB IS networks;
c) Logging activities of administrators and systems operators (must be done separately);
d) Logging and reporting of updates (version, configuration) of the system components used in the management of the alerts monitoring.

The preventive maintenance of these elements must be logged and associated with alert subject to corrective action.

Collaboration platform logs must be at least secured as BoostAeroSpace data and protected following the same rules. Extra protection shall be added to prevent high privilege accounts modification of logs integrity.

The log recording time period must not be less than 1 year and must comply with applicable laws.

## 7. Control of identity and access to the BAS infrastructure

*(UsMgr, Users)*

Note: Each partner owns and is responsible for the data that he store on the platform BoostAeroSpace.

The administration of a partner's user's rights is the responsibility of the partner.

[2] On the purchase of Hub Services

| | |
|---|---|
| *(User, SP)* | **7.1. Business requirements for access control to the BAS infrastructure**<br>*Objective: To control access to information.*<br>- Guideline:<br>All access to data or systems is assigned individually and strictly according to, on one hand, the need to know basic in regards of user function, and, on the other hand, the right to know. |
| *(User)* | - Rules:<br>The need to know is defined by the line manager of the user. |
| *(User)* | The right to know is defined by the data owner. |
| *(SP) to (SMA)* | Access to data and systems are being:<br>a) strong individual identifications and authentications, regardless of the type of access (user and administrator) and the origin of the connection;<br>b) traceability of access on the one hand, and actions on data on the other hand, these accesses must be auditable in accordance with procedures defined by the SMA (see § 11.2 "Compliance with policies and security standards"). |
| *(CISO) to (SMA)* | The document Hub *Access Control policy [RD10]* is written by HUB security officer and must be approved by the SMA. This document is based on the following:<br>a) hub Identity and Access strictly formal Control Policy;<br>b) document managed by the Hub Security Officer, updated & monitored periodically by the SMA;<br>c) integration of principles and rules of access management defined in the following chapter. |
| *(SP)* | **7.2. Access Management**<br>*Objective: Control access of authorized users and prevent unauthorized access to information systems.*<br>- Access login credentials<br>The access to BAS infrastructure devices (network, systems) is individualized. It must **always** be done by certificate authentication allowing to uniquely identifying one and only one individual. |
| *(President)* | In case of certificate authentication the BoostAeroSpace Certification Authority is responsible the uniqueness of names of subscribers and the resolution of disputes concerning the claim of a name usage.<br>Hub resources access identification rules are specified in the document *"Hub Access Control Policy" [RD08].*<br>These rules govern all access uses cases (personal of BoostAeroSpace, users, service providers). |

| | |
|---|---|
| | - Users identity repository<br>The Hub repository of identities is created & updated from partner's users' identity management repositories of their employees & suppliers. It is the responsibility of the owning entity (source) of the user to manage individual information, including:<br>• the validity period of the account (based on user identifier)<br>• User access profile validated by the partner in the case of a provider (need to know basis).<br>The repository of identities of the Hub must allow establishing the relationship between the resource access user identifier and company affiliation of the person. |
| *(President)* | In case of strong authentication, the publication of the certificate of authentication (registration authority) or the certificate request to the competent authority must be recorded. |
| *(UsMgr, SP)* | - Registration and deregistration of users<br>The procedures for registration / deregistration and revocation of access rights for users are governed by the principles below.<br>When user leave it's owning entity:<br>• its access to the hub must be removed immediately (by revocation of his certificate by the source entity in case of certificate authentication); |
| *(UsMgr, SP)* | • All application access rights must be locked immediately;<br>• The deletion of the account access to the hub and access rights to applications must be effective after a time period, whose duration must be specified in the *Hub access control policy [RD08]*, given that only identity information are kept for HUB traceability purposes. |
| *(SP)* | Moreover, the account will be suspended if idle more than three months. A new account unused for over a month will also be suspended. |
| *(CISO) to (SMA)* | These procedures are owned by the HUB security officer, responsible for their definition and maintenance. They must be available to all stakeholders, approved in advance by the SMA and auditable. |
| *(SP) to (SMA)* | - Systems privilege management<br>The administration of systems and networks is ensured by entities validated by the SMA. |
| *(SP)* | The security requirements for administration are subject to specific rules explained in particular in the *Hub access controls policy [RD08].* They are enforceable by the administrators and must be subject to their individual commitments. |

| | |
|---|---|
| | These requirements include the following:<br>a) the operations and management of systems, databases and networks are made in standard with individual & personal account with limited privileges, reserved specifically for this purpose.<br>b) all access and actions carried out with highly privileges accounts must receive enhanced monitoring and traceability,<br>c) the accumulation of privileges on the different types of components (networks - systems - security) of the hub by a single individual is strictly prohibited and the principle of separation of privileges is applied,<br>d) the keeping of a register and escrow of default products systems highly privileges accounts and its reporting to the SMA on request.<br>e) the periodic updating of default products systems highly privileges accounts passwords and the service accounts (default and / or shared use) when changing function;<br>f) the personals having theses HUB highly privileges accounts under their responsibility must have first signed an associated privacy and security commitment, including also:<br>o compliance with the rules applicable to the management and use of highly privilege accounts |
| *(SP)* | |
| *(SP) to (SMA)* | o a duty to alert the SMA on incident and / or anomalous security event. |
| *(User, UsMgr, SMA)* | - <u>Identity Management:</u><br>Each end user must be granted a secured credential that allow her to be identified uniquely directly by the credential or by the owner of the credential.<br>The security level of the credential shall be adapted to the sensitivity of the data accessed by the user or the sensitivity of the actions he is allowed to perform.<br>In case of certificate authentication, the certificate must be issued by a Certification Authority recognized and approved by the SMA. |
| *(President)* | - <u>Cross-certification:</u><br>The principle of cross-certification of the hub relies on conformity to practices from the certification policy (CP) of Certification Authorities (CA) issuing certificates in regards of practices from the BoostAeroSpace cross certification CA policy [RD04]. |

## 7.3. Liability of HUB members and their users

*Objective: To prevent access by unauthorized users, the compromising or theft of information and means of information processing*

*(User, UsMgr)*

Referring to the commitment of the user [RD09], members of the Hub must ensure that their HUB users and administrators have well signed their acceptance of *the acceptable terms of usage of the HUB [RD09],* and they must provide the associated evidence.

HUB members must also allow users to be able to meet the proper application of these procedures and the rules of the *Hub Access Control Policy [RD08].*

As such, the *acceptable terms of usage of the HUB [RD09]* and the *Hub Access Control Policy [RD08]* must specify the specific rules relating to the following:

a) the use of identification means;
b) materials left under no direct survey;
c) clean desk and blank screen policy.

## 7.4. Internet network access control

*Objective: To prevent unauthorized access to services available on the Internet*

*(SP)*

Regarding access to the Internet from the HUB:

The Hub BoostAeroSpace must provide access to the strict services and applications validated [RD14] of BoostAeroSpace Hub.

Accordingly, once authenticated to the BoostAeroSpace platform, the accessing cannot reach other external information systems as applications and services validated [RD14].

*(User, UsMgr)*

Regarding the HUB access from Internet:

a) The access from the Internet to the portal is considered for a HUB user category provided with business company Internet compliant with this security policy.
b) BoostAeroSpace platform is only accessible from the **Secured portal**.

The *Hub access controls Policy document [RD08]* will include information on the terms and rules of the following policies:

c) the use of network services;
d) User authentication for external connections;
e) identification of equipements used in networks;
f) protection for diagnosis and remote configuration ports;
g) the partitioning of networks;
h) measures relating to the connection of networks;
i) control of network routing.

## 7.5. Operating systems access controls

*Objective: To prevent unauthorized access to operating systems*

Access to operating systems in the scope of the Hub must be protected. Their access controls must comply with enforced monitoring.

*(CISO) to (SMA)*

The *Hub access controls Policy document [RD08]*, achieved by the Hub Security officer, and validated by the SMA must therefore specify the operational security devices used to:

a) the opening of secured sessions;
b) identification and authentication of entities accessing to these systems;
c) management of authentication methods;
d) the use of system utilities;
e) the automatic disconnection of idle sessions.

## 7.6. Applications and data access control

*(CISO) to (SMA)*

*Objective: To prevent unauthorized access to information stored in applications*

Depending on the *HUB classification of information & applications [RD06]* and the respect of the need to know basic, the *Hub access controls Policy document [RD08]* achieved by the Hub Security officer and validated by the SMA must reserve a special section for access control to applications and data according to their sensitivity.

## 7.7. Nomads access

*(CISO)*

*Objective: Ensure information security when using mobile computing devices.*

The *Hub access controls Policy document [RD08] must* reserve a special section on mobile computing specifying that the company providing access to the HUB from the mobile terminal of the user undertakes to respect the HUB Security policy.

*(User, UsMgr)*

This section must contain particular requirements regarding:

a) antivirus protection of terminals (any device connecting to the hub must have an anti-virus with up to date virus signatures);
b) security of the terminals (intrusion protection, absence of dual networks connection, firewall, encryption, timeouts);
c) Supported Operating Systems patch management including security patches management;
d) Measures of source device access control (identification / authentication).

## 7.8. Remote administration

*(SP) to (SMA)*

*Objective: Specify the rules applicable to remote maintenance equipment of the HUB.*

Remote administration on BoostAeroSpace collaborative platform service will be authorized only after specific SMA validation of security controls.

| | |
|---|---|
| *(SP)* | Remote operators must be authenticated using BoostAeroSpace compliant PKI credentials protected on hardware tokens.<br>Only IPSEC VPN connection or equivalent will be authorized.<br>Remote operations must be logged for 6 month, if possible administrator activities shall be recorded for 1 month and administrators must be explicitly identified in the logs of the operated device. Logs & activity records must be available on SMA re-quest on a 3 days outlook basis. |
| *(SP) to (CISO)* | Remote site must be audited by BAS CISO or by SMA validated third party as compliant with the BAS Security Policy. |

# 8. Information systems acquisition, development and maintenance

## 8.1. Information systems security requirements

*Objective: To ensure that security is an integral part of information systems*

The evolution of operating systems, their operation and their organization can change the security problematic and require changes in operating procedures.

The Hub must ensure with the help of the SMA the proper maintaining of security level defined by this security policy. The consequences can lead to the implementation of preventive measures to avoid regressions of security.

*(SP) to (SMA)*

Any development of application is managed as a project with the writing of specifications answering security requirements. This implies that the different phases of validation before deployment include the verification of compliance with these security requirements and the non-security regression in the case of evolution by the SMA.

Any changes and / or project must be associated with:

a) As a minimum of 1 (one) security review before entry into service;
b) 1 (one) vulnerability audit, as soon as the changes are significant and may impact partners data security before entry into service.

Major changes (as for example, "infrastructure network design modification", "hosting provider change", etc.) shall be associated with evaluation against Advanced Persistent Threat (APT) and targeted attacks at least 6 months after the first entry into service and on a regular basis, at least every 3 years. The evaluation shall be performed by security experts capable to simulate attack over the services as a skilled team of hackers would perform, taking into account the level of gain of a successful attack to determine the level of the simulated attack. The service provider shall be capable to show, after the evaluation, the capability of its security infrastructure to detect and stop the attack.

Periodic audits conducted under the supervision of the SMA, must allow detection of residual risks that may affect the hub information system.

For all the security evaluations, the service provider shall comply with evaluation reports risk analysis rules for resolution of identified issues: as soon as possible for major issues, 6 (six) months for major issues, 1 (one) year for observations.

### 8.2. Development and application operations

*Objective: To ensure the software security with separation of production environments with other environments.*

*(SP)*

Development environments must observe the following rules:

a) be separated from production environments;
b) do not contain BoostAeroSpace operational production data;
c) allow to ensure the security of development environments within the framework defined in this security policy.

*(SP) to (SMA)*

The separation between BoostAeroSpace production and development environments must be auditable by the SMA.

## 9. Security incidents management

### 9.1. Information events and weaknesses reporting

*(SP) to (CISO)*

*Objective: Ensure the method of reporting incidents and vulnerabilities related to information security to enable the implementation of corrective action as soon as possible.*

*then*

*(CISO) to (SMA)*

The existence and the activation of a system for reporting incidents and vulnerabilities related to Information security contribute to Hub security. This information must be raised by the BoostAeroSpace security officer to the SMA in accordance with the procedure of HUB incident management & escalation [RD10].

This document [RD10] must precise:

a) The obligations of alert feedback to the HUB security officer from service providers in terms of content and delay;
b) The raising of security alert to hub customers when necessary;
c) Commitments to the implementation of corrective measures by service providers and / or customers (immediate action and corrective action plan)

### 9.2. Events management

*Objective: Ensure implementation of coherent and effective approach for the management of events relating to information security.*

*(SP) to (SMA)*

A procedure for managing events written by each services provider will be approved by the SMA and must include:

a) A procedure for events raising;
b) An escalation procedure by event classification;
c) A procedure and an organization for crisis management;
d) Process of collecting and preserving evidences;
e) An experience feedback capitalized and integrated into existing procedures.

## 10. Business Continuity

*(President) to (SMA)*

*Objective: To prevent disruption of the organization's activities, protect critical business processes from the effects caused by major failures of information systems or disasters and ensure a recovery of these processes as soon as possible.*

BoostAeroSpace must submit to SMA validation:

a) the systems solutions to ensure business continuity in production, according to Service Level Agreement (SLA) (backup / services recovery operations);
b) Safety plan & Disaster Recovery Plan (DRP) [RD11] specifying the acceptable period of inactivity defined by the steering committee of BoostAeroSpace.

*(SP) to (SMA)*

The test results of the annual DRP will be communicated to the SMA.

## 11. Compliance

*(President) to (CISO)*

*then*

*(CISO) to (SMA)*

The conformity control actions of Hub Security will integrate methodically, in the implementation of this policy, the control points listed below.

These checkpoints will be followed with one hand, under the recurring management of security by BoostAeroSpace security officer, under the supervision of the SMA, and with other hand, through periodical compliance or vulnerability audits requested by the SMA and executed in the confines of the Hub information system.

## 11.1. Compliance with legal requirements

*Objective: Avoid any violation of legal, statutory, regulatory or contractual obligations and security requirements.*

BoostAeroSpace must ensure that hosting providers and third parties comply with legal requirements of the hosting country and country of origin to HUB access.

Monitoring compliance with legal requirements involves taking into account at minimum when applicable the following items (list to be completed according to the laws of the countries concerned) and Company procedures to answer.

*(CISO, SP)*

List of items subject to compliance monitoring:

a) the explicit definition, documented and up to date for all regulatory, legislative and contractual constraints;
b) intellectual property rights, usage of software licenses and associated appropriated procedures against legal, regulatory and contractual usage constraints;
c) protection of valuable information against loss, destruction and falsification, in accordance with legal, regulatory, contractual and professional constraints;
d) protection and confidentiality of personal data in accordance with legislation and contractual terms;
e) prevention among users to not use the infrastructure of information processing for illegal matters;
f) the use of cryptography in compliance with laws, agreements between the members (if existing) and regulations in force in the country where it is implemented.

## 11.2. Compliance with policies and security standards

*(PRESIDENT)*

*Objective: To ensure system compliance with security policies and standards of the organization*

BoostAeroSpace must ensure that the practices and policies of hosts providers and third parties are in accordance with what is stated in this document.

*(SP) to (CISO)*

*then*

*(CISO) to (SMA)*

The compliance monitoring with policies and security standards involves the periodic inspection by the BoostAeroSpace security officer among service providers on the following:

a) all security procedures are executed properly in accordance with the Hub Security Policy and security standards;
b) operational audits of HUB security constraints application are performed by each service provider within the various information systems;
c) security reporting is achieved;
d) this control will be conducted at a minimum once a year and will be written in a report submitted to the validation of the SMA, which can, according to, commission an audit.

# 12. APPENDIX

## 12.1. Appendix 1 - Reference documents

| REFERENCE DOCUMENTS | | | | |
|---|---|---|---|---|
| *List of reference documents "during the rally Used - column" Index "= reference to Be Used In The text (eg. [RD01])* | | | | |
| **Index** | **Title & filename (with url or rental)** | **Owner** | **Issue** | **Date** |
| [RD01] | Rules of usage and operation of assets | BAS | TBW | |
| [RD02] | Trust_Security_Baseline | BAS | 1.5 | 26/10/10 |
| [RD03] | Boost AeroSpace Security Policy | BAS CISO | 1.1 | 20/11/12 |
| [RD04] | Boost Bridge Certificate Policy | BAS | 1.2 | 13/09/11 |
| [RD05] | BoostAeroSpace SMA Charter | BAS | 1.1 | 20/09/11 |
| [RD06] | BoostAeroSpace classification of information | BAS | 1.0 | 28/02/12 |
| [RD07] | Hub actor identification fundamentals | BAS | TBW | |
| [RD08] | Hub Access Control Policy | BAS CISO | TBW | |
| [RD09] | BoostAeroSpace acceptable use policy for users & administrators | BAS | 1.2 | 06/02/12 |
| [RD10] | HUB incident management procedure | BAS CISO | TBW | |
| [RD11] | Activity Recovery Plan (PRA) | BAS CISO | TBW | |
| [RD14] | BAS HUB validated applications and services list | BAS CISO | TBW | |
| [RD15] | BoostAeroSpace Backup Global policy | BAS | TBW | |