Security Policy Update
Modifications from v1.2 to V1.3

Document's target audience:

This document intended to all BAS HUB users or candidate to join the BAS HUB that will manipulate data from and / or to the HUB.

This includes BAS hub services end users, infrastructures administrators and guest users.

Modifications executive summary:

Policy regarding services providers' evaluation of the security against Advanced Persistent Threats:

The paragraph of the Chapter 8.1 "Information systems security requirements" dealing with Service providers' obligations and responsibilities toward the security management of its services has been detailed regarding the security assessments that service providers shall perform.

It has been requested to service provider to perform cyber-attack simulations on its services after entry into service and show evidences of the capability of the service provider to detect and stop such attacks.

The obligations in terms of resolutions of the issues discovered during those security evaluation as well as during the BoostAeroSpace Security Management Authority (SMA) mandated audits has also been more detailed in terms of delay in regards of the severity of the issues.

BoostAeroSpace executive committee vs president references:

The references inside the Policy regarding the former executive committee body has been replace with "President" structure, following the change of BoostAeroSpace governance that happened in January 2015.

25/09/2016

Detailed modifications:

1. Modification 1

Paragraph(s) and page(s) number(s):

- Chapter 8.1 “8.1. Information systems security requirements”, P20.

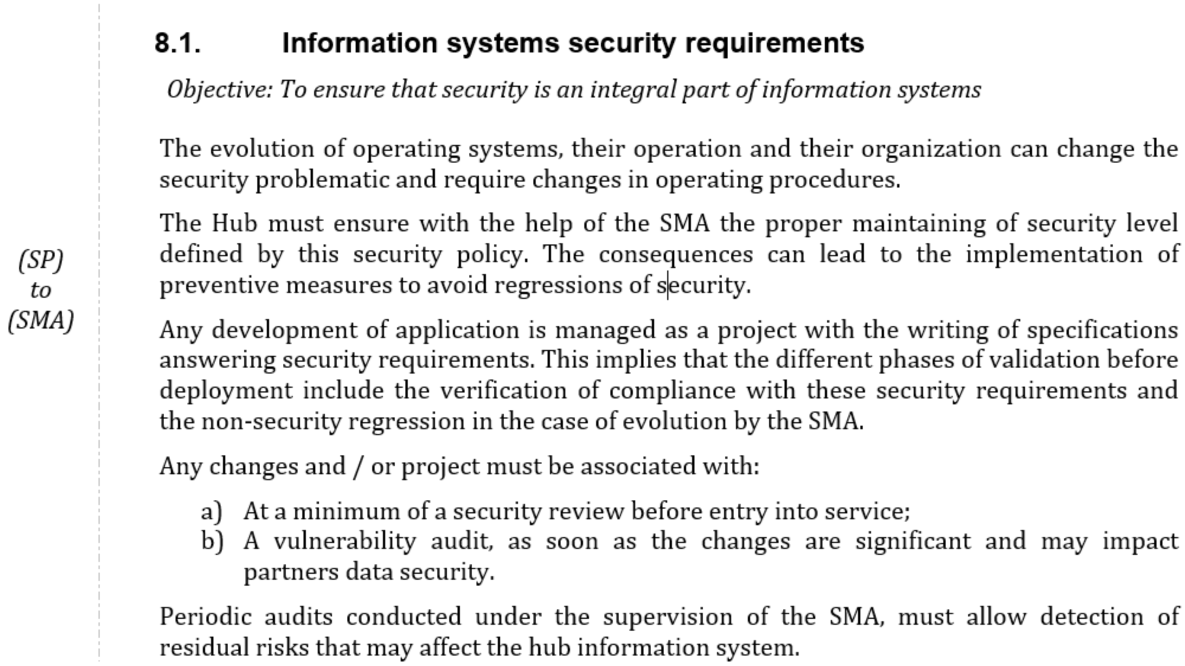
Modification summary:

The paragraph of the Chapter 8.1 “Information systems security requirements” dealing with Service providers’ obligations and responsibilities toward the security management of its services has been detailed regarding the security assessments that service providers shall perform.

It has been requested to service provider to perform cyber-attack simulations on its services after entry into service and show evidences of the capability of the service provider to detect and stop such attacks.

The obligations in terms of resolutions of the issues discovered during those security evaluation as well as during the BoostAeroSpace Security Management Authority (SMA) mandated audits has also been more detailed in terms of delay in regards of the severity of the issues.

Previous Security Policy 1.2 extract:



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.

(SP) to (SMA)

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.

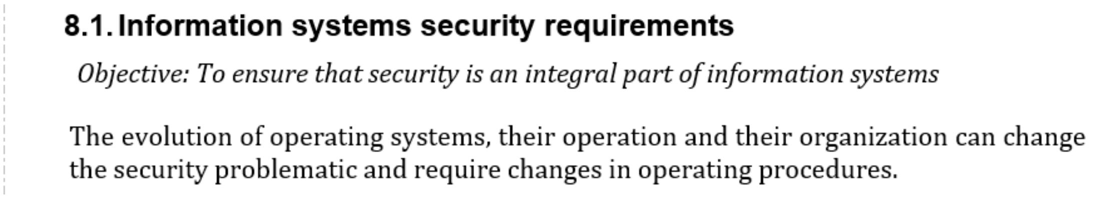
Any development of application is managed as a project with the writing of specifications answering security requirements. This implies that the different phases of validation before deployment include the verification of compliance with these security requirements and the non-security regression in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

Any changes and / or project must be associated with:

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

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

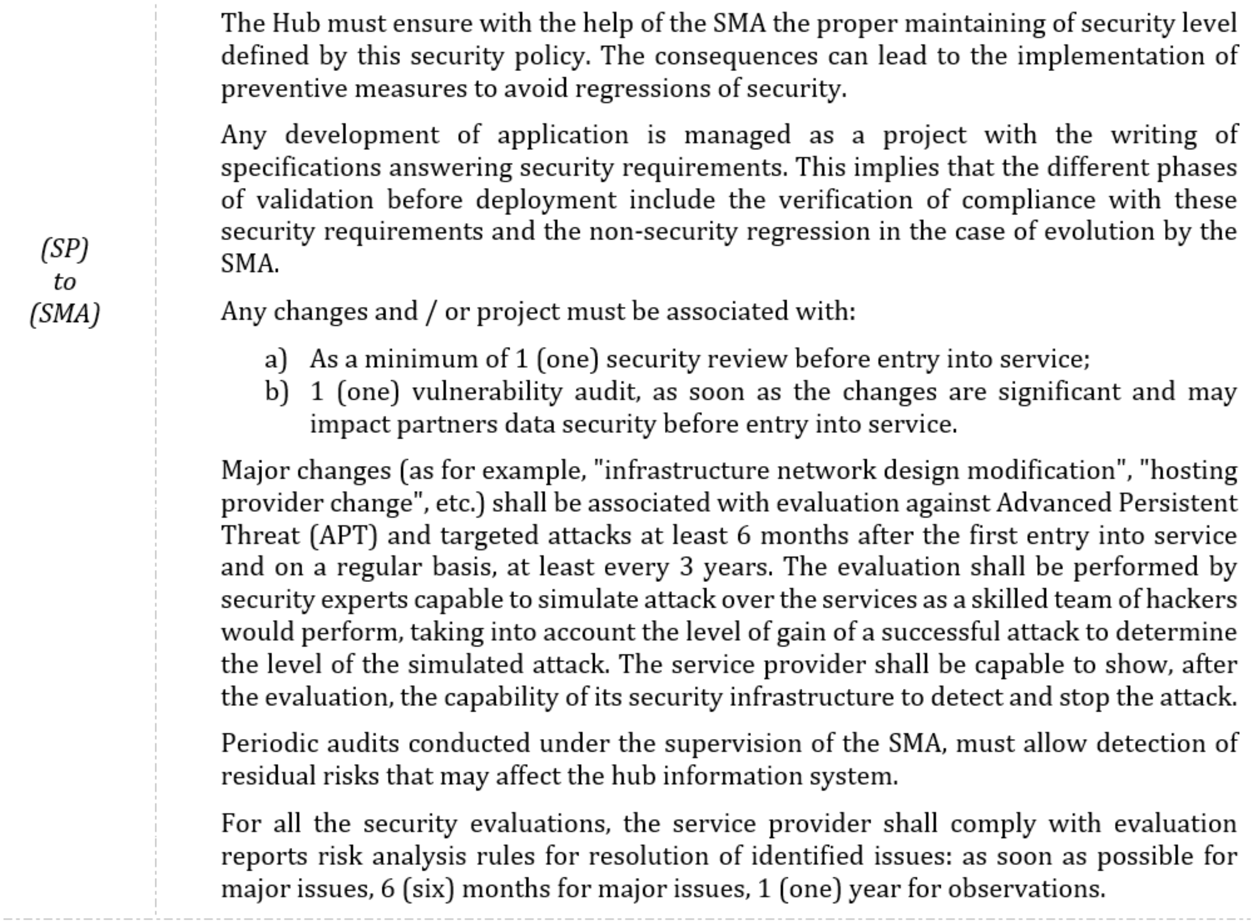
New Security Policy 1.3 extract:



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.



(SP) *to* *(SMA)*	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. 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.

2. Modification 2

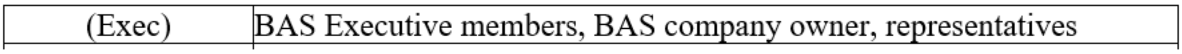
Paragraph(s) and page(s) number(s):

All document.

Modification summary:

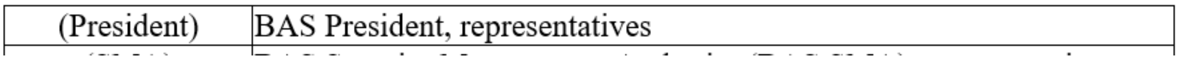
The references inside the Policy regarding the former executive committee body has been replace with "President" structure, following the change of BoostAeroSpace governance that happened in January 2015.

Previous Security Policy 1.2 extract:



(Exec)	BAS Executive members, BAS company owner, representatives

New Security Policy 1.3 extract:



(President)	BAS President, representatives