

Brio Access and Data Security Policy 2.1 “Brio ADS Policy”

OID:1.3.6.1.4.1.10438.2.1

Historique

Version	Date	Author	Description
1.0	13/11/2006	C. Cloesen	1 st official version
1.1	13/11/2006	C. Cloesen	
1.2	13/11/2006	C. Cloesen	
1.3	13/11/2006	C. Cloesen	
1.4	1/12/2015	COMDIR	Alignment with the other ADS policies
2.0	24/05/2016	PortiSign™ Steering Committee	Added GDPR in 10. Compliance
2.1	1/7/2016	Ulys	Added article 5.5

Table of contents

1.	DEFINITIONS AND ACRONYMS	4
2.	OVERVIEW	6
3.	POLICY ADMINISTRATION.....	7
3.1	ORGANIZATION ADMINISTERING THE DOCUMENT.....	7
3.2	CONTACT PERSON	7
3.3	DISTRIBUTION OF THE BRIO ADS POLICY	7
4.	LOGICAL ACCESS TO THE APPLICATION	8
4.1	PRINCIPLES	8
4.2	VALID DIGITAL IDENTITIES.....	8
4.3	ACCREDITED CERTIFICATES AUTHORITIES	8
4.4	VALID PASSWORDS	8
4.5	AUTHENTICATION	8
4.6	AUTHORIZATION.....	8
4.7	LICENSE CONTROL.....	9
4.8	CONTROLS FOR BROKERS ON MS WINDOWS ENVIRONMENTS	9
4.9	SESSION RESTRICTION	9
4.10	APPLICATION ACCESS CONTROL COMPONENTS.....	9
4.11	APPLICATION MAIN COMPONENTS ACCESS CONTROLS	9
5.	DATA SECURITY.....	10
5.1	DATA BACKUP AND BUSINESS RESUMPTION PLANS	10
5.1.1	<i>Data backup.....</i>	<i>10</i>
5.1.2	<i>Disaster Recovery Plan Site ("DRP Site").....</i>	<i>10</i>
5.2	DATA CONFIDENTIALITY	11
5.3	DATA INTEGRITY	11
5.4	DATA PRIVACY	11
5.5	NATIONAL REGISTRATION NUMBER	11
6.	PHYSICAL AND OPERATIONAL REQUIREMENTS	12
6.1	PHYSICAL CONTROLS	12
6.1.1	<i>Application Access Control Components.....</i>	<i>12</i>
6.1.2	<i>Application Main Components including files and databases.....</i>	<i>12</i>
6.2	POWER AND AIR CONDITIONING	12
6.3	CABLING SECURITY	12
6.4	WATER EXPOSURES	12

- 6.5 FIRE PREVENTION AND PROTECTION 12
- 6.6 MEDIA STORAGE 12
- 6.7 OFF-SITE BACKUP 13
- 6.8 WASTE DISPOSAL 13
- 7. LOGGING, MONITORING, INCIDENT RESPONSE, AUDITING..... 14**
 - 7.1 LOGGING AND MONITORING 14
 - 7.2 INCIDENT RESPONSE..... 14
 - 7.3 REMOTE ACCESS 14
 - 7.4 ESCALATION PROCEDURE..... 14
 - 7.5 AUDITING 14
- 8. PROCEDURAL CONTROLS 16**
 - 8.1 TRUSTED ROLES 16
 - 8.2 NUMBER OF PERSONS REQUIRED PER TASK..... 16
 - 8.3 ROLES REQUIRING A SEPARATION OF DUTIES 17
- 9. PERSONNEL CONTROLS 18**
 - 9.1 TRAINING REQUIREMENTS 18
 - 9.2 SANCTIONS FOR UNAUTHORIZED ACTIONS 18
 - 9.3 INDEPENDENT CONTRACTOR REQUIREMENTS 18
 - 9.4 DOCUMENTATION SUPPLIED TO PERSONNEL 18
- 10. COMPLIANCE 18**

1. DEFINITIONS AND ACRONYMS

Access Holder	Designates the physical person or organization who undertakes the Application-related contractual relationship with Portima. The Access Holder will be granted access to the Application upon signature of this agreement. The Access Holder is the interlocutor of Portima for all aspects related to the Application.
Application	Refers to a management and production software dedicated to insurance brokerage offices and remotely accessible. Its commercial names are Brio Startup, Brio Classic, Brio and <i>Brio Plus</i> , grouped under the brand name Brio.
Application Access Control Components	Designates the set of hardware, software, telecommunication systems that are responsible for controlling authentication, authorization and licensing functionalities of the Application.
Application Main Components	Designates the set of hardware, software, telecommunication systems that are responsible for providing functionalities included in the Application by processing the data owned by the Access Holder.
Application Service Provider (ASP)	Designates Portima as its role of Application supplier. The Application is hosted on servers owned and operated by Portima, or on servers owned and operated by Portima's accredited chosen subcontractor.
Authorized Users	Designates physical persons that were granted access to the Application by the Access Holder. The usage of the Application made by Authorized Users is done under the name and responsibility of the Access Holder.
Broker Contact Center (BCC)	Portima team providing support and assistance to brokers regarding applications such as Brio and their usage.
Certificate Authority (CA)	A CA is a collection of hardware, software, and the people who operate it. The CA performs four basic operations: <ul style="list-style-type: none"> • Issues certificates (i.e., creates and signs them) for the Registration Authorities, Local Registration Authorities, End Users, and Entities (those last 3 cover the roles of Access Holders and Authorized Users) • Maintains certificate status information and issues Certificate Revocation Lists (CRLs) • Publishes certificates and Certificate Revocation Lists (CRLs) • Maintains archives of status information about expired or revoked certificates that it issued.
Certificate Policy (CP)	A named set of rules that indicate the applicability of a certificate to a particular community and/or class of application with common security requirements.
Certification Practice Statement (CPS)	A statement of the practices, which a Certification Authority employs in issuing certificates.
Consumer	Client of a broker, gaining access to a restricted set of data within the Brio database, corresponding to his/her insurance context, or to any other set of Brio data deemed as relevant by the Access Holder, directly, or indirectly by the Authorized Users under the supervision of the Access Holder.
Data	Designates the set of files (text or other formats) generated during the use of the Application by the Access Holder or the Authorized Users.
Digital identity	Refers to a digital avatar of the physical identity of a person.
Document Management System	Set of hardware (servers, storage) and software components designed to allow authorized users to store and retrieve a large number of documents (PDF, Word, e-mails, ...), in a reliable, fast and secure way.
Hosting	Designates the fact to allocate disk space and computer resources in order to store and process data.
MyBroker	Set of applications on various platforms that allow Consumers to view their granted subset of Brio data, and interact with the broker by performing some transactional tasks. MyBroker rely on the Brio infrastructure and data.
Portima Security Officer (PSO)	Portima employs Security Officers whose principle role is the security of their domain of responsibility (network, PKI, etc.).
Public Key Infrastructure (PKI)	Set of hardware, software, people, policies and procedures needed to create, manage, store, distribute, and revoke certificates. A PKI is based on public-key cryptography.

Secure Production Area	Protected computer rooms where the servers and network components are hosted at Portima's (or Portima-appointed subcontractor's) premises, including the DRP site
-------------------------------	---

2. OVERVIEW

Portima is responsible for the development and hosting of a software application that delivers management and production functionalities for a broker office. This application is remotely accessible and the four available versions are named BRIO (Broker Remote Insurance Office), BRIO*startup*, BRIO*classic* or BRIO*plus*. It is referred hereafter as the “Application” or Brio.

“Application” or Brio also applies to mobile applications dedicated to brokers, using Brio application as back-end.

For Consumers, the Brio application can also serve as a management and back-end system for the MyBroker applications on various platforms; however, even if many of the policy statements described below still apply, MyBroker applications for consumers are ruled by a specific policy “MyBroker Access and Data Security Policy” (OID: 1.3.6.1.4.1.10438.2.2)

This document covers the security aspects related to Access Control and Data Security in the Application and is named “Brio Access and Data Security Policy” (referred as “Brio ADS Policy” hereafter).

This Brio ADS Policy should be read in combination with the applicable contractual documentation and any other Documents it may refer to.

The IANA OID of this document is 1.3.6.1.4.1.10438.2.1

<http://www.iana.org/assignments/enterprise-numbers/enterprise-numbers>

3. POLICY ADMINISTRATION

3.1 Organization Administering the Document

Portima maintains, registers, revises, and interprets this Brio ADS Policy.

3.2 Contact Person

All questions and comments concerning Brio ADS Policy should be addressed to:

Christophe Cloesen
Portima Chief Information Officer
Chaussée de la Hulpe 150
1170 Bruxelles
Belgium
Tel: +32 (0)2 661 44 11
Fax: +32 (0)2 661 44 49
Email: security@portima.com

3.3 Distribution of the Brio ADS Policy

The Brio ADS Policy shall be available to all participants who intend to use this environment. This Brio ADS Policy can be retrieved in either of the following ways:

- Distribution via publishing on the Portima web site, within Portima applications; or
- Distribution via e-mail.

4. LOGICAL ACCESS TO THE APPLICATION

4.1 Principles

Login services shall provide for positive authentication that will ensure that only Authorized Users are allowed access to the Application.

Authorized Users that are successfully authenticated shall then undergo an authorization control phase that will check for actual access rights into the Application, and for license checking.

4.2 Valid digital identities

In order to get access to the Application, an Authorized user shall possess a digital certificate, issued by a Portima-accredited Certificate Authority (CA) and registered by the Access Holder in the Authorized Users database.

4.3 Accredited Certificates Authorities

Portima recognizes as trusted CA:

- Portima Certificate Authority (OID 1.3.6.1.4.1.10438.1) ruled by the Portima Certificate Policy (CP) and implemented as described in the Certification Practice Statement (CPS) (OIDs: 1.3.6.1.4.1.10438.1.1 and 1.3.6.1.4.1.10438.1.2)
- PortiSign Certificate Authority (OID 1.3.6.1.4.1.10438.3) ruled by the PortiSign CP and implemented as described in the CPS (OIDs: 1.3.6.1.4.1.10438.3.1 and 1.3.6.1.4.1.10438.3.2)
- Belgian Citizen CA, responsible for certificates on eID cards (ruled by OID:2.16.56.1.1.1.2, OID:2.16.56.1.1.1.2.1, OID:2.16.56.1.1.1.2.2, OID:2.16.56.9.1.1.2, OID: 2.16.56.9.1.1.2.1,OID: 2.16.56.9.1.1.2.2)

PortiSign CA is accepted solely in the MyBroker context.

4.4 Valid passwords

Each corresponding private key of a digital certificate granting access to the Application, issued by Portima CA, shall be protected by its own password. A valid password shall be a combination of letters, numbers, and/or special characters; be at least 6 characters long. For other digital certificates, issued by Portima or by Third Parties, the related password policy and constraints supersede the former.

4.5 Authentication

In order to successfully authenticate to the Application, an Authorized User shall at least undergo:

- a validity check on the digital certificate validity period,
- a validity check against appropriate revocation lists,
- a validity check against administrative suspension of the Authorized User requested by the Access Holder.

4.6 Authorization

In order to pass the positive authorization controls, an Authorized User shall at least undergo:

- A belonging check to the Authorized Users community provided by the Access Holder,

- A control on the actual ownership of access rights granting access to the Application and to its specialized modules.

4.7 License control

An Authorized User, after having been successfully Authenticated and Authorized, will be submitted to the license control. This control is made with respect to the terms and conditions described in the contract ruling the relationship between the Access Holder and Portima. A successfully logged-in Authorized User might be denied access to the Application or get a stripped-down access rights set to the Application, if maximum licensed access rights are exceeded.

4.8 Controls for Brokers on MS Windows environments

All PCs and servers using MS Windows are checked against the presence of an active antivirus program. If no active antivirus is detected, the access to the Application will not be granted. The signature definition of the antivirus program shall be up to date.

4.9 Session restriction

In order to protect the logged-in sessions to the Application, Authorized Users shall log off or lock (activate the password-protected screensaver of) their workstations when not in use.

4.10 Application Access Control Components

Network connections to and from these components are protected through encryption and firewalls.

4.11 Application Main Components Access Controls

Network connections to and from these components are protected through firewalls.

5. DATA SECURITY

5.1 Data backup and business resumption plans 5.1.1

Data backup

As an application provider, Portima has implemented systems and processes to ensure the continuity of business and integrity of data. As a minimal backup scenario¹, daily database backups are performed to be able to restore the system to a known baseline. These backups are kept under strict configuration control and stored off-line in a secure facility.

Documents are stored in a separate Document Management System, which is backed up using a specific backup scheme: documents are immediately replicated to the Primary DRP site, and synchronized daily to a Secondary DRP Site. Other controls are in place². Access to archived data is restricted by a control list of screened personnel.

5.1.2 Disaster Recovery Plan Site (“DRP Site”)

The Application has a redundant architecture (including e.g. telecom lines, redundant hardware, load balancing-capable software). A functionally identical Application system is maintained in another, distant, hosting site to support business resumption.

The effectiveness of this Primary DRP Site and the associated recovery procedures are at least tested once a year, e.g. for each Brio major release, or by performing specific tests, cf. Portima Business Continuity Strategy.

Portima operates and maintains a Secondary DRP Site in order to insure the maximal availability of the Application. The Application at this site is configured in such a way that the data pertaining and processed by the Application cannot be changed by the Access Holder or the Authorized Users.

The Access Holder can refuse to subscribe to this additional service. In order to formally decline this service, the Access Holder has to sign off an opt-out form, available at the Portima Infoline, and return it to Portima. Upon receipt, Portima has to remove the data of the Access Holder from the secondary DRP Site within 7 working days.

¹ Detailed backup plan:

	Frequency	Retention
Data-redo logs	24 times per day, every day	1 week
Data	1 time per week (full backup)	2 weeks
Data	1 time per day every day (incremental backup)	1 week
Data	1 time per month (full backup)	3 months
Data	1 time per quarter (full backup)	1 year
Operating System & Application	1 time per day (incremental backup)	1 week
Operating System & Application	1 time per week (full backup)	1 month

² Documents written in Brio are written simultaneously to the Brio database and to the Document Management System and retained in databases for at least 3 months. Documents in the Brio database are kept long enough to perform coherence check between the 4 environments: Brio database, Document Management System in Production, primary DRP site and secondary DRP site. This coherence check happens at least on a weekly basis. Documents on the secondary DRP site are backed up on a monthly basis. Deletion of documents on the production environment is delayed by 13 months on the Secondary DRP Site.

For those two DRP Sites, physical and logical data access protection is guaranteed as equivalent to the Production environment, and this applies for both actual data and backup data.

5.2 Data Confidentiality

The confidentiality of the data is ensured within the Application as only Authorised Users can access it.

5.3 Data Integrity

Portima implements security controls to ensure the integrity of data within the Application.

5.4 Data Privacy

Some of the information processed by the Application shall be considered as personal data, following applicable privacy/data protection legislation. If not implicit (e.g. legislation compliance), formalization of this "personal data" classification can be done by any method deemed appropriate (e.g. contract, NDA, ...).

5.5 National registration number

Some personal data are governed by dedicated regulation. This is notably the case of the National Registration Number (NRN) (see the Act of 8 August 1983). This NRN is however mandatory when a broker wants to submit a request to register a vehicle at the competent administrative authorities (DIV). To minimize legal risks, the NRN is subject to limitations in the Application. Such limitations include notably a prohibition to use the export tools of the Application in relation to the NRN, as well as encryption of this data. Such limitation applies as long as the contract is in force as well as at the end of the contract.

6. PHYSICAL AND OPERATIONAL REQUIREMENTS

6.1 Physical Controls

6.1.1 Application Access Control Components

The infrastructure for Application Access Control Components resides in the secure production area at Portima's (or Portima-appointed subcontractors') premises.

Physical access to these hardware components, networks and information are restricted to designated Portima (or Portima-appointed subcontractor's) employees on a need to know basis. Changes to the Application Access and Data Security Components require the presence of at least two individuals.

6.1.2 Application Main Components including files and databases

The infrastructure for the Application Main Components (including files and databases) resides in the secure production area at Portima's (or Portima-appointed subcontractor's) premises.

Physical access to these hardware components, networks and information are restricted to designated Portima (or Portima-appointed subcontractor) employees on a need to know basis. Access to the hosting area is submitted to accreditation, automatic authorization control and logging.

6.2 Power and air conditioning

Servers in the secure production area at Portima's (or Portima-appointed subcontractor's) premises are protected against power outage. These servers are connected to an Uninterruptible Power Supply (UPS).

Stable temperatures for the Application Access Control Components and Application Main Components hardware equipment are guaranteed by an air conditioning (AC) system. The AC is installed in such a way that it will not reduce the physical security of the room nor compromise the functioning of the hardware/software.

6.3 Cabling Security

Telecommunications cables are protected against interception or damage within the secure production area at Portima's (or Portima-appointed subcontractor's) premises.

6.4 Water exposures

The secure production area is protected from water damage by its design, using a raised floor.

6.5 Fire prevention and protection

Policies regarding fire prevention, detection and protection are applied.

6.6 Media storage

Portima has a place, both on-site and off-site, to store backups and distribution media that prevents loss, tampering, or unauthorized use of the stored information. Backups are kept both for data recovery and archival of important information.

6.7 Off-site backup

Off-site backups benefit from at least the same level of physical security than on-site backups. Backup files stored off-site through deduplication techniques and remote synchronization also benefit at least from the same level of logical and network security as on-site backups. Removable backups media are sealed by Portima or appointed subcontractor staff before leaving Portima's or appointed subcontractor's premises.

6.8 Waste disposal

All servers, computers and drives are checked to ensure that any sensitive information related to the Application has been removed or overwritten prior to disposal.

A shredder is used to destroy sensitive Application information written or printed on paper.

7. LOGGING, MONITORING, INCIDENT RESPONSE, AUDITING

7.1 Logging and Monitoring

Security audit procedures apply to all computer/system components, which host the Application Access Control Components and the Application Main Components.

Portima Security Officer aims at keeping up-to-date with relevant information security standards and being aware of security related issues to ensure compliance with these procedures.

Security incidents as well as any access to the Application are logged. Audit trails provide a mechanism for recording and subsequently tracing the actions of individuals. Hence, recorded information includes the identity of the individuals performing any action to access the information and the time of access.

Portima assesses the security posture and vulnerabilities of its information systems at its premises on an ongoing basis. Portima Security Officer analyses the log-files and can add other events to be logged in order to improve security tracking.

7.2 Incident Response

Security incidents including complaints from the brokers related to the security of the Applications or infrastructure provided by Portima are logged and tracked in a central system (Broker Contact Center (BCC)).

7.3 Remote access

For incident resolution out of normal business hours, Portima IT staff (e.g. engineers, administrators) might have to remotely get access to the Application infrastructure and network. This is done via a secure VPN connection.

7.4 Escalation procedure

Portima Security Officers can initiate the escalation procedure. It includes three types of remediating actions, based on the level of incident:

- Organizational actions such as the implementation of segregation of duty;
- Operational actions such as a change in the operating procedures;
- Technical actions such as the replacement of a server.

7.5 Auditing

Portima performs regular security audit of its IT infrastructure and Applications in order to assess:

- Its security posture
- Its compliance with laws and regulations

These audits include:

- Automated tests (e.g. vulnerability scans)
- Manual tests performed by independent auditors

- Compliance audit performed by independent auditors
- Penetration tests performed by independent auditors

Independent auditors can either be Portima employees not involved in the development, implementation or operational maintenance of the systems tested or independent third party security experts.

Before putting into production a new online service for the brokers, Portima performs some functionality and security testing beforehand and retest the systems prior any major release.

Whenever audits are externalized, Portima provides relevant information and access to the independent third party, as needed to perform the audit.

Third party security experts performing audits must only communicate testing results to Portima employees or subcontractors, designated by Portima CIO, on a need to know basis, since testing results are confidential information.

Auditors are responsible for the integrity of testing results.

Auditors should never jeopardize the security of online services while performing their tests. Testing should be transparent to brokers and any other users of Portima Applications and infrastructure.

8. PROCEDURAL CONTROLS

8.1 Trusted Roles

This section describes the roles and responsibilities of the different Application Access Control Components and Application Main Components.

Identified specific roles:

- **Access Holder:** He is owner of the data, and as such:
 - o He is the sole person who can designate Authorized Users that will get access to the Application and is consequently responsible for all transactions made within the Application by the Authorized Users.
 - o He is the sole person who can request, register or revoke digital identities linked to the Authorized Users. Those actions cannot be repudiated afterward by the Access Holder.
 - o He is the sole person who can change internal access rights to specific actions within the Application.
- **Authorized User:** He can access the Application with the appropriate level of access rights granted by the Access Holder.
- **Portima or Portima-appointed subcontractor system engineer or operator:** He designs, installs, configures, maintains systems supporting the Application. He does not have access to data. He knowingly and formally agrees to comply with this policy, including the personnel controls chapter (see § 9)
- **Portima or Portima-appointed subcontractor operator:** He monitors and operates systems supporting the Application and related batch processes. He does not have access to specific data. He knowingly and formally agrees to comply with this policy, including the personnel controls chapter (see § 9)
- **Portima or Portima-appointed subcontractor data administrator:** he is responsible for all aspects related to data files and databases management in the Application. He has access to data, but he is not authorized to access or manipulate specific data unless formally authorized by the Access Holder. He knowingly and formally agrees to comply with this policy, including the personnel controls chapter (see § 9)
- **Portima BCC staff:** BCC staff might be asked by the Access Holder for remote or on-site assistance. In this case, the Access Holder or his/her delegates might ask for joined problem resolution once logged in the Application. A conscious approval (technical action) should be given by the Access Holder or his/her delegates. In some cases, for further investigations, it might be required to get a copy of the production data of the Access Holder.
- **Portima Analyst:** Portima Analyst might take over problems that cannot be solved by Portima BCC staff. In this case, for further investigations, it might be required to get a copy of the production data of the Access Holder. This requires a formal approval of the Access Holder (see below for more procedural details)
- **Portima Security Officers:** Beyond eventual roles described in Portima Certificate Policy, Portima Security Officers are responsible for the analysis of the security logs and security audits of their respective domain. They recommend actions to Portima management upon detection of a threat or unaddressed risk.

8.2 Number of persons required per task

Dual or multiple control principle is applied where necessary and suitable.

8.3 Roles Requiring a Separation of Duties

As a minimum, operations that require a separation of duties are:

- Installation, upgrade of software systems that support the Application (e.g. split roles like documenting changes/instructions and actually applying them)
- Physical access to the systems that support the Application
- Investigation on bugs or questions submitted by the Access Holder. Specifically for this point:
 - o The Access Holder must provide Portima BCC staff with a formal approval form.
 - o A Portima Analyst has to validate the actual suitability of getting the production Application data from the Access Holder.
 - o A Portima System Engineer has to verify that all the conditions above are respected and then will request a backup of the production Application data from the Access Holder.
 - o A Portima Analyst will analyze the production Application data from the Access Holder and will, if appropriate, propose a solution that might affect the production Application data from the Access Holder.
 - o A Portima System Engineer will delete all temporary data that was used during the investigation process.

9. PERSONNEL CONTROLS

9.1 Training requirements

Each Portima or appointed subcontractor staff member working with the Application receives the appropriate training allowing him/her to perform his/her tasks in a knowledgeable and secure way.

9.2 Sanctions for unauthorized actions

Cf Portima Information Security Policy section 7 .

9.3 Independent contractor requirements

Cf Portima Information Security Policy section 15.

9.4 Documentation supplied to personnel

Each Portima staff member or Portima-appointed subcontractor staff member working with the Application receives relevant documents describing their responsibilities and duties. These documents are supplied only on a need-to-know basis.

10. COMPLIANCE

The rules defined in this document take into consideration the security requirements for Brio accesses and data, based upon:

- Business-driven needs expressed by the different stakeholders involved
- Best security practices

Besides those drivers, applicable regulations as well as Belgian and European laws are taken into consideration and will prevail in case of conflict. In particular:

- Legal Circular of FSMA (CBFA-2009-17 of 7th March 2009)
- Legal Circular Annex of FSMA (CBFA-2009-17-1 of 7th March 2009), in particular the chapter 3.2.1
- Act of 8th December 1992 on the protection of privacy (consolidated version 7/04/2014)
- Belgian legislation on data retention (30/07/2013)
- EU General Data Protection Regulation (GDPR) – For practical information see Portima Information Security Policy