ISMS – Rules for ICT suppliers

TABLE OF CONTENTS

1 SCOPE

This procedure lists rules for all suppliers that access or use Air Dolomiti S.p.A. information.

For ICT suppliers, a special document is available.

2 DEFINITIONS AND ACRONYMS

Air Dolomiti S.p.A. information are all confidential.

They include any information, in tangible or intangible form, that is proprietary or confidential to Air Dolomiti S.p.A. and is disclosed to the supplier, including, without limitation, trade secrets, know-how, computer programs and software, specifications, design plans, drawings, data, prototypes, customer information, passenger information or other business and technical information, without regard to whether it is disclosed in oral, written, electronic, visual or other form.

3 RESPONSIBILITIES

ICT: manage this document

Controlling & Internal Auditing: controls its enforcement.

Managers: require to suppliers to enforce the rules in this document.

Suppliers: enforce rules in this document, according with the scope of their work.

4 GENERAL RULES

4.1 Purpose of information processing

Information processing by the supplier must be limited to the scope of work. No other purposes is allowed.

4.2 Confidentiality agreement

All Air Dolomiti S.p.A. information are confidential and of Air Dolomiti S.p.A. ownership.

Air Dolomiti S.p.A. information cannot be communicated to anyone if not authorized by Air Dolomiti S.p.A. Care must be given to the identification of the receiver (e.g. telephone calls by someone declaring to be an Air Dolomiti S.p.A. representative, market researchers, journalists, customers).

As general rule, the supplier ensures that all risks (either accidental or deliberated) of non-authorized access, dissemination, integrity and availability, regarding Air Dolomiti S.p.A. information are properly addressed.

4.3 Employees management

Employees include permanent staff, temporary staff, contractors, interns, etc.

The supplier ensures that it has with all employees a confidentiality agreement and set rules for ensuring confidentiality of information, including Air Dolomiti S.p.A. ones.

4.4 Sub/Supplier management

The supplier can use sub-suppliers.

The supplier maintains a list of sub-suppliers with their processing scopes. The supplier ensures to Air Dolomiti S.p.A. the right to access this list, if needed for legal compliance purposes.

The suppliers ensures that it has, on contractual agreements, the same information security provisions with all its sub-suppliers that access Air Dolomiti S.p.A. information.

4.5 Audit

The supplier ensures to programme, plan and perform audits in order to verify the effectiveness of implemented technical and organizational information security controls.

The supplier ensures to Air Dolomiti S.p.A. the right of audit, given an announcement of at least 3 weeks in advance. Air Dolomiti S.p.A. representative will not ask to access other customers information.

4.6 Exchange of Air Dolomiti S.p.A. information

For exchanging Air Dolomiti S.p.A. digital documentation, only Air Dolomiti S.p.A. file sharing systems can be used or password protected files.

When Air Dolomiti S.p.A. documents (digital or hardcopies) are read, the user must verify that no unauthorized people can read them.

When Air Dolomiti S.p.A. information are exchanged in conversation, persons must verify that no unauthorized people can hear them.

4.7 Incident management

The supplier ensures to Air Dolomiti S.p.A. that it will communicate as soon as possible any information security event or vulnerability (digital or not digital) to Air Dolomiti S.p.A.

The supplier ensure all assistance when requested by Air Dolomiti S.p.A. in case of information security incidents or vulnerabilities.

4.8 Contract ending

The supplier ensures the deletion or destruction of all Air Dolomiti S.p.A. information when closing the contract.

The supplier ensures, at the end of the contract, the handover to Air Dolomiti S.p.A. designated people or organizations.

5 ACCESS TO AIR DOLOMITI S.P.A. SYSTEMS

This clause applies if the supplier can access to Air Dolomiti S.p.A. IT systems.

5.1 I&A to Air Dolomiti S.p.A. IT systems

Air Dolomiti S.p.A. userid and password are intended for internal use only in your organization and:

- cannot be shared with any other organizations;
- must be preserved so that no one can discover it;
- password must be modified if there is any suspect that someone else knows it

Password are set with defined criteria:
- length at least 8 characters;
- complexity (at least one small cap letter, one capital letter, one number, one symbol);
- change no later than every 90 days.

5.2 ICT devices for accessing Air Dolomiti S.p.A. information

For accessing Air Dolomiti S.p.A. documentation, only personal or company devices can be used (e.g. it is forbidden to use Internet points).

IT devices such as pcs, smartphone and removable media must be secured:
- access controlled with user id and password as mentioned before;
- updated antimalware;
- software patched and updated according to the latest vendor hints;
- secure Air Dolomiti S.p.A. data deletion when no more needed.

If mobile devices are used, all Air Dolomiti S.p.A. data are securely deleted as soon as possible and the device is never exchanged with not-authorized people if Air Dolomiti S.p.A. data are still available on it.

6 COMMUNICATION WITH AIR DOLOMITI S.P.A.

Communication with Air Dolomiti S.p.A. is authorized only through agreed channels. Ticketing tools, where users are personally identified are the preferred choice.

A list of people authorized by Air Dolomiti S.p.A. and the supplier is exchanged and updated when necessary.

7 DATA PROTECTION

The Parties will comply at all times with the requirements of the Data Protection Laws.
The supplier Company acknowledges that under the terms of this Agreement:

it will act as a Data Processor (appointed by Air Dolomiti S.p.A. who is a Data Controller);

it will have access to Personal Data in respect of which Air Dolomiti S.p.A. is Data Controller.

The supplier Company undertakes that it will only process Personal Data as necessary in relation to the provision of the Services as set out in this Agreement and in particular will:

- not pass the Personal Data to any third party if not authorized;
- keep the Personal Data confidential;
- perform its obligations in accordance with the Data Protection Law applicable and particularly the data protection Principles;
- comply with Air Dolomiti S.p.A. systems or procedures which Air Dolomiti S.p.A. may introduce from time to time in respect of the processing of the Personal Data, including the Data Protection Policies.

The supplier Company will act in accordance with all reasonable instructions from Air Dolomiti S.p.A. in respect of the processing of Personal Data.

The supplier Company warrants that it has in place appropriate technical and organisational security measures against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data.
The supplier Company will provide Air Dolomiti S.p.A. with such information as is reasonably necessary to enable Air Dolomiti S.p.A. to satisfy itself of the supplier Company's compliance with this privacy clause.
The supplier Company agrees not to process Personal Data outside of the European Economic Area (or any other country deemed adequate by the Commission pursuant to Article 25(6) of Directive 95/46/EC) without the prior written consent of Air Dolomiti S.p.A..
For the avoidance of doubt the Parties acknowledge that all Personal Data is the property of Air Dolomiti S.p.A..
The supplier Company agrees to notify Air Dolomiti S.p.A. immediately:

- if it cannot comply with its obligations under this clause;
- about any accidental or unauthorised access;
- about any legally binding request for disclosure of the personal data by a law enforcement agency unless otherwise prohibited under criminal law; and
- about any request received directly from the data subjects without responding to the request unless it has been authorised to do so.

On termination of provision of the Services, the supplier Company shall, at the choice of Air Dolomiti S.p.A., either return all Personal Data transferred and copies thereof; or secure destroy all Personal Data and certify that it has done so.

8 SYSTEM AND NETWORK MANAGEMENT

Rules in this chapter are enforced by suppliers that host or manage servers or ICT networks.

8.1 Server configuration

For servers, virtual machines, storage, DBMS and network devices configuration, the following rules are applied as appropriate:

- if possible, the default administration user-id is not used and disabled;
- servers, virtual machines, storages, DBMS and devices have access controlled with credentials:
    - unique user-id for each users;
    - password length at least 8 characters;
    - password complexity enforced requiring small and capital letters, numbers, special characters (e.g.: @, #, !);
    - expiration after no more than 90 days;
    - history of at least 5 passwords (the user cannot use the previous used passwords);
- servers, virtual machines, storages, DBMS and devices are connected, if possible, with Air Dolomiti S.p.A. Active Directory, Centrify or Radius for authorization;
- there are at least two administrators in order to ensure continuity of operations;
- servers and devices are connected with the NTP server;
- unused and potentially dangerous services on servers and devices are disabled or uninstalled;
- remote access is allowed only through VPN;

- administrators login and logout are collected and protected (internal servers and devices are connected with Air Dolomiti S.p.A. tools);
- connection with performance monitoring tools;
- install and test with Air Dolomiti S.p.A. HP Data Protector backup agent;
- potential vulnerabilities are monitored in order to apply patch, fixes or workaround as soon as possible, within six months on availability;
- if the installation of critical or security patch, fixes fails then an internal HDA ticket is created;
- antimalware software is installed with automatic updates on whenever possible and linked with Air Dolomiti S.p.A. central Sophos console;
- any installation is done according to the change management procedure (see below);
- development and test servers are segregated from production ones;
- when hard disks are no more used for Air Dolomiti S.p.A., they are securely formatted.

8.2 Network and network devices

For network configuration, the following rules are applied:

- all network devices are hardened:
  - only secure connections (e.g. TLS, SSH, HTTPS, SFTP) are allowed; all others (e.g. Telnet) are disabled;
  - insecure protocols are disabled (e.g. SNMP, at least outside internal network);
  - access is only with personal accounts (eg: root or local admin are not permitted);
  - connections are only through certificates or similar mechanisms wherever applicable;
- all connections outside internal network are encrypted;
- IT services with access from external parties are on a DMZ; whenever possible, services are protected by a proxy;
- IPSEC VPN has a time limit (no longer than one year);
- systems exposed on the Internet have the minimum installed services and are loosely coupled with other services, in order to be quickly updated when patches and fix are available;
- potential vulnerabilities are monitored in order to apply patch, fixes or workaround as soon as possible, within six months on availability;
- if the installation of critical or security patch, fixes fails then an internal HDA ticket is created;
- access from the Internet is only through cryptographic channels;
- internal network is segmented as appropriate (e.g. DB, application server, DMZ, client and management networks) with VLANS or firewall;
- internal network is separated from Internet with firewalls;
- devices are redundant as applicable;
- when the device is no more used for Air Dolomiti S.p.A., hard disks are securely formatted.

For firewalls:

- an integrity test of the programs and files installed is regularly performed (at least once a month);
- rules and configurations are regularly checked, at least once a year.

8.3 Asset inventories

An asset inventory is always available for Air Dolomiti S.p.A., with:

- physical servers and virtual machines;
- applications, services, middleware and DBMS, linked with VMs;
- network devices.

8.4 Change management

All changes with potential impacts on Air Dolomiti services, must be previously authorized by Air Dolomiti.

For applications, no changes in production system is authorized if not tested in test environment before.

8.5 Data centre and cabling

The following rules are applied for Data centre(s) where Air Dolomiti S.p.A. devices are housed:

- physical access control is enforced, if possible access control is based on personal badge;
- anti-intrusion alarms are installed;
- automatic smoke detection is installed;
- fire extinguishers (automatic or manual) are available;
- temperature sensors are installed and alarms are configured;
- air conditioning is installed and maintained (air conditioning is redundant for critical data centres);
- redundant power supply is ensured by UPS and generators;
- cables for power and data are segregated from each other and in pipelines;
- cables for data transmissions are labelled;
- cabling is redundant.

Mechanisms are maintained according to a maintenance programme.

9 APPLICATION DEVELOPMENT

The following are ensured by the supplier that design and develop applications for Air Dolomiti.

If any of the following is not enforced, concession from Air Dolomiti must be required before the deploy of the project.

9.1 Development environment requirements

Development environment requirements:

- When possible, tests are done with fake data, not copies of production ones; if copies of real data are used, access control is enforced;
- All code is controlled with a configuration and version control mechanism;
- Development environments are secured by: access control, backups, remark of activities;
- Connections between development and test servers and production servers are never set up with writing authorization in production;
- Tests (at least integration tests) are performed by different people than developers.

9.2 Documentation requirements

Documentation requirements are the following:

- Security functions (including applicable laws and regulations) are documented;
  - including details how to configure cryptographic modules (algorithms, key length);
- Security architecture (including system and network) is documented;
- in case of source code given to Air Dolomiti,
  - the standard used for naming classes, method, functions, variables and constants is available;
  - rules for coding are available for Air Dolomiti;
- Security tests are documented (misuse cases);
- Functional test are documented (including the requirements of this document);
- Technical tests are documented (including the requirements of this document);
- System tests are documented (including the requirements of this document);
- Vulnerability assessment have been performed and documented;
  - for web applications, vulnerability assessment based on OWASP Top 10 have been performed and documented.

9.3 Security functions

The following security functions are considered in the application and relevant documentation:

- Data protection security functions, as required by applicable laws and regulations (e.g. privacy) are implemented (Privacy by design and Privacy by default);
- Users are authenticated with user-id and password (or a central system, e.g. Active Directory, is used);
- Password strength is automatically controlled:
  - 8 characters long;
  - use of letters (capital and not capital), numbers and special characters;
  - history of at least 5 passwords (the user cannot use the previous used passwords);
- The system requires the users to change the password every 90 days;
- Passwords are masked in login field;
- Roles and profiles can be set according with Air Dolomiti needs;
- Users don’t need administration privileges;
- Transmission on external networks are always encrypted with secure protocols (e.g. with TSL 1.2 with AES 256 and RSA 2048);
- In case of databases, users cannot access to data, only to application;
- For critical actions (e.g. deletion), users actions require confirmation by the users;
- The system ensure the collection of System administrators logs about:
  - login and logout;
  - critical changes;
- User actions are logged (insert, changes and deletion of information);
- Capacity (e.g. maximum number of users) has been tested through stress tests;
- The system is scalable;
- All errors are managed and messages to users don’t give too much information about the system;
- Database server is encrypted (not mandatory).

9.4 Security technical requirements

The following Security technical requirements are considered in the application and relevant documentation:

- For web application: input data (including URL, HTTP headers, cookies) are sanitized (e.g. type, max, min, length, special characters) before elaboration by the server;
    - Note: sanitization covers at least OWASP Top 10 vulnerabilities.
- Inputs use a valid character set (e.g. UTF-8);
- Credentials (user-id and password) are verified only on server;
- Credentials are never cached on clients (and never, e.g. on cookies, URL);
- In case of databases: databases ensure referential integrity;
- Transactions are always verified for integrity (e.g. check digits, duplications, ACK);
- Concurrent transactions are managed.

9.5 System requirements

The following System requirements are considered in the application and relevant documentation:

- System is on three tiers: db, application (on internal network) and presentation (on DMZ);
- Connection with other systems follows the minimum privilege principle;
- No connection with other systems requires administration privileges;
- Connection with other systems, if based on passwords, requires passwords of at least 16 characters;
- Connection with other systems is based on digital certificates (not mandatory)
- The NTP can be configured.

9.6 Coding requirements

The following Coding requirements are considered in the application and relevant documentation:

- Software is modular: each module performs only one function (cohesion);
- Access control modules are segregated from other functional modules;
- Software objects are loose coupled;
- Data are not coded in software objects (including configuration files, service passwords);
- Each user or administration operation is controlled for its authorizations before commitment (complete mediation)

9.7 Mobile apps requirements

The following Mobile apps requirements are considered in the application and relevant documentation:

- The app requires the minimum number of permissions to users;
- Memory used by the app is not shared with other apps;
- “Quit” or “Logout” buttons are clearly visible to users in all pages;
- Sessions expires after a defined time period;
- No credentials are in the code;
- Transmissions of data (including passwords) are always encrypted (AES 256, RSA 2048);

- Data (including passwords and crpyto keys) stored on the device is encrypted (AES 256);
- Debug and reverse engineering is prevented (obfuscation).

9.8 Maintenance requirements

The following are ensured during maintenance:

- Changes are recorded on a configuration system and authorized by Air Dolomiti;
- System provider ensure the availability of updates in case of vulnerabilities;
- Changes in development, test and production systems can be done in different phases;
- If external software, libraries, APIs are used, vulnerability patches are monitored and available to users;
- For maintenance, supplier or other people can access with personal user-ids (not shared credentials).

10 PRIVACY BY DESIGN AND PRIVACY BY DEFAULT

The Privacy by Design (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after. Whether applied to information technologies, organizational practices, physical design, or networked information ecosystems, PbD begins with an explicit recognition of the value and benefits of proactively adopting strong privacy practices, early and consistently (for example, preventing (internal) data breaches from happening in the first place).
The suppliers should underscribe the following guidelines.

10.1 Privacy as the Default

We can all be certain of one thing − the default rules! Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy − it is built into the system, by default.
This PbD principle, which could be viewed as Privacy by Default, is particularly informed by the following Fair Information Practices:
 Purpose Specification – the purposes for which personal information is collected, used, retained and disclosed shall be communicated to the individual (data subject) at or before the time the information is collected. Specified purposes should be clear, limited and relevant to the circumstances.
 Collection Limitation – the collection of personal information must be fair, lawful and limited to that which is necessary for the specified purposes.
 Data Minimization − the collection of personally identifiable information should be kept to a strict minimum. The design of programs, information and communications technologies, and systems should begin with non-identifiable interactions and transactions, as the default. Wherever possible, identifiability, observability, and linkability of personal information should be minimized.
 Use, Retention, and Disclosure Limitation – the use, retention, and disclosure of personal information shall be limited to the relevant purposes identified to the individual, for which he or she has consented, except where otherwise required by law. Personal

information shall be retained only as long as necessary to fulfill the stated purposes, and then securely destroyed.
Where the need or use of personal information is not clear, there shall be a presumption of privacy and the precautionary principle shall apply: the default settings shall be the most privacy protective.

10.2 .Privacy Embedded into Design

Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.
Privacy must be embedded into technologies, operations, and information architectures in a holistic, integrative and creative way. Holistic, because additional, broader contexts must always be considered.
Integrative, because all stakeholders and interests should be consulted. Creative, because embedding privacy sometimes means re-inventing existing choices because the alternatives are unacceptable.
 A systemic, principled approach to embedding privacy should be adopted − one that relies upon accepted standards and frameworks, which are amenable to external reviews and audits. All fair information practices should be applied with equal rigour, at every step in the design and operation.
 Wherever possible, detailed privacy impact and risk assessments should be carried out and published, clearly documenting the privacy risks and all measures taken to mitigate those risks, including consideration of alternatives and the selection of metrics.
 The privacy impacts of the resulting technology, operation or information architecture, and their uses, should be demonstrably minimized, and not easily degraded through use, misconfiguration or error.

10.3 Full Functionality – Positive-Sum, not Zero-Sum

Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum “winwin” manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretence of false dichotomies, such as privacy vs. security, demonstrating that it is possible, and far more desirable, to have both.
Privacy by Design does not simply involve the making of declarations and commitments − it relates to satisfying all legitimate objectives − not only the privacy goals. Privacy by Design is doubly-enabling in nature, permitting full functionality − real, practical results and beneficial outcomes to be achieved for multiple parties.
 When embedding privacy into a given technology, process, or system, it should be done in such a way that full functionality is not impaired, and to the greatest extent possible, that all requirements are optimized.
 Privacy is often positioned in a zero-sum manner as having to compete with other legitimate interests, design objectives, and technical capabilities, in a given domain. Privacy by Design rejects taking such an approach – it embraces legitimate non-privacy objectives and accommodates them, in an innovative positive-sum manner.
 All interests and objectives must be clearly documented, desired functions articulated, metrics agreed upon and applied, and trade-offs rejected as often being unnecessary, in favour of finding a solution that enables multi-functionality.
Additional recognition is garnered for creativity and innovation in achieving all objectives and functionalities in an integrative, positive-sum manner. Entities that succeed in

overcoming outmoded zero-sum choices are demonstrating first-class global privacy leadership, having achieved the Gold Standard.

10.4 End-to-End Security – Lifecycle Protection

Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, secure lifecycle management of information, end-to-end.
Privacy must be continuously protected across the entire domain and throughout the life-cycle of the data in question. There should be no gaps in either protection or accountability. The “Security” principle has special relevance here because, at its essence, without strong security, there can be no privacy.
 Security − Entities must assume responsibility for the security of personal information (generally commensurate with the degree of sensitivity) throughout its entire lifecycle, consistent with standards that have been developed by recognized standards development bodies.
 Applied security standards must assure the confidentiality, integrity and availability of personal data throughout its lifecycle including, inter alia, methods of secure destruction, appropriate encryption, and strong access control and logging methods.

10.5 Visibility and Transparency

Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to both users and providers alike. Remember, trust but verify!
Visibility and transparency are essential to establishing accountability and trust. This PbD principle tracks well to Fair Information Practices in their entirety, but for auditing purposes, special emphasis may be placed upon the following FIPs:
 Accountabilty – The collection of personal information entails a duty of care for its protection. Responsibility for all privacy-related policies and procedures shall be documented and communicated as appropriate, and assigned to a specified individual. When transferring personal information to third parties, equivalent privacy protection through contractual or other means shall be secured.
 Openness – Openness and transparency are key to accountability. Information about the policies and practices relating to the management of personal information shall be made readily available to individuals.
 Compliance – Complaint and redress mechanisms should be established, and information communicated about them to individuals, including how to access the next level of appeal. Necessary steps to monitor, evaluate, and verify compliance with privacy policies and procedures should be taken.

10.6 Respect for User Privacy

Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric!

The best Privacy by Design results are usually those that are consciously designed around the interests and needs of individual users, who have the greatest vested interest in the management of their own personal data.
Empowering data subjects to play an active role in the management of their own data may be the single most effective check against abuses and misuses of privacy and personal data. Respect for User Privacy is supported by the following FIPs:
 Consent – The individual's free and specific consent is required for the collection, use or disclosure of personal information, except where otherwise permitted by law. The greater the sensitivity of the data, the clearer and more specific the quality of the consent required. Consent may be withdrawn at a later date.
 Accuracy – personal information shall be as accurate, complete, and up-to-date as is necessary to fulfill the specified purposes.
 Access – Individuals shall be provided access to their personal information and informed of its uses and disclosures. Individuals shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
 Compliance – Organizations must establish complaint and redress mechanisms, and communicate information about them to the public, including how to access the next level of appeal.
Respect for User Privacy goes beyond these FIPs, and extends to the need for human-machine interfaces to be human-centered, user-centric and user-friendly so that informed privacy decisions may be reliably exercised. Similarly, business operations and physical architectures should also demonstrate the same degree of consideration for the individual, who should feature prominently at the centre of operations involving collections of personal data.