Lantik BFA DFB Bizkaiko Foru Aldundia Diputación Foral de Bizkaia	NCS-1 / 2

Data Security Regulations for Suppliers

Prepared and updated by: Security Department	Reviewed by: 01
	Effective date: 02/05/2011

1. PURPOSE	2. SCOPE
This document seeks to establish the data security regulations applicable to the Lantik service providers	Lantik service providers.

CONTENTS

3. Data Security for Lantik

The importance of Data Security for Lantik

Information, along with the people, processes, systems, networks, etc.., that support it, are considered to be important assets. The availability, integrity, confidentiality, authentication and traceability of the information and the supporting assets are fundamental to ensure data security, compliance of current legislation, competitiveness and to protect a good corporate image in the eyes of the clients.
Managing the information is essential to achieve appropriate data security. It has to be underpinned by appropriate regulations and procedures to be fulfilled by any individuals that use Lantik assets in order to carry out their work.

Goals of the Data Security Regulations

The overall goals of the Data Security Regulations are as follows:

- ***Legal Framework***

  The suppliers shall undertake to **comply with current legislation** regarding the protection and safety of the information and the systems applicable to all their business processes.

- ***Legislative Framework***

  Compliance of the contractual obligations established with clients and suppliers regarding data security.

  Compliance of the Data Security requirements and good practice included in ISO27001 and ISO27002 standards.

4. Organisation, reviewing and updating legislation

This legislation shall be reviewed periodically. However, given the very evolution of technology, threats relating to data security and to the relevant new legal obligations, Lantik hereby reserves the right to amend this legislation when necessary. Any changes made shall be disseminated to all interested parties by means of publishing the new version on the Lantik website and circulating it by email by the CAU. Any person who carries out activities for Lantik is responsible for reading, knowing and complying with this Data Security Legislation for Suppliers.

5. Breach of the Data Security Regulations

Lantik hereby reserves the right to adopt any measures that it considers relevant regarding the contract company and which may even involve terminating the contracts in force with that company.

6. Organisational aspects of data security

Objectives

- To ensure the data security of the Lantik data assets accessed, processed, communicated or managed by service providers.

1. Suppliers

.1 The agreements (contracts) that imply accessing, processing, disseminating or managing the information of the organisation or the data processing services, or adding products or services to the data processing services, shall envisage the security checks required by Lantik prior to the service provision.

7. Asset management

Objectives

- To establish and ensure appropriate protection of the Lantik assets.
- To ensure that the data receives an appropriate level of protection.

1. Accountability regarding the assets

.1 The supplier shall comply with the standards for the acceptable use of the assets established by Lantik in its data security management.

Internal Standard NCS-1/1 Security Standard: Computer Code of Conduct for Suppliers

2. Data classification

.1 **All the information related to Lantik activities is considered to be confidential.** The supplier shall comply with all the functions and obligations regarding the use of the data system according to Lantik regulations.

.2 The handling of the data shall be guaranteed pursuant to the established classification criterion.

8. Environmental and physical security

Objectives

- To prevent and stop unauthorised access, damage and interference to the Lantik facilities and data.
- To protect the Lantik system, by locating them in areas protected by a defined security perimeter, with security measures and appropriate access controls.
- To contemplate the protection of the Lantik systems, when transferring and establishing them outside the secure areas, for maintenance or other motives.
- To control the external factors or of the environment that could endanger the correct operating of the data systems that host the Lantik information.

- To implement measures to protect the data handled by employees, in the normal framework of their standard tasks.

1. Secure areas

.1 The physical entry controls shall be used correctly. They have been established to ensure that only authorised personnel access the Lantik areas: premises, offices and installations.

.2 The suppliers shall follow the Lantik protection guidelines and measures regarding possible environmental and external threats.

.3 The suppliers shall comply with the guidelines established for working in the protected areas.

.4 The identification card used by the suppliers shall be clearly visible while on Lantik premises.

2. Equipment security

.1 The technological infrastructure shall be located on secure and protected sites in order to reduce the risks from external threats.

.2 The technological infrastructure shall be protected, where applicable, against power failures.

.3 The connection of any hardware to the electrical and communication circuits shall be previously authorised, in order to avoid interceptions or damage.

.4 Prior authorisation shall be requested and the indicated control measures shall be implemented, particularly with regard to the infrastructure that for specific reasons has to be located outside the protected areas at Lantik or outside the organisation.

.5 Except in those cases when express updates are received, no ICT infrastructure or software belonging to Lantik may be taken off the premises.

9. Operations and communications management

Objectives

- To guarantee the correct and secure operating of the assets that the different services supply to Lantik.
- To establish accountabilities and facilitate management and operation procedures, including operating instructions, procedures for the response to incidents and separation of functions.

1. Accountabilities and operating procedures

.1 Lantik shall facilitate, according to the identified needs, updated operating procedures to the suppliers that need them.

.2 Changes may not be made to the infrastructures and the resources.

.3 Areas of responsibility and tasks shall be defined in a segregated manner in the contracts and in the service agreements established, in order to avoid any unauthorised changes.

.4 The correct use of the testing and development environment shall be guaranteed, according to the service provided by the supplier.

2. Service provision management

.1 Lantik shall conduct checks to verify that the security requirements established prior to the service provision have been implemented and are still in place.

.2 The provided services shall be monitored and reviewed periodically. Depending on the type of service, compliance audits may be required.

.3 According to the critical nature and/or risk of the contracted service, changes to its provision shall be authorised by Lantik beforehand.

3. Scheduling and acceptance of the system

.1 The use by the supplier of the resources belonging to Lantik shall be supervised in order to guarantee their correct capacity both in the present by means of their monitoring and in the future by means of trends analysis.

.2 Acceptance criteria shall be established for new systems or modification to existing systems, by suppliers. Tests will be carried out in the development and testing environment in order to ensure a smooth move to the production stage. Migration to the production environment will only take place after the formal acceptance.

4. Protection against downloadable and malicious code

.1 Running unauthorised code is forbidden. The configuration of the hardware shall guarantee that the authorised code runs according to what is defined in the relevant regulations.

5. Managing network security

.1 The Lantik management activities and mechanisms to protect against any threats to the networks and the applications that they use may not be deactivated.

.2 The security characteristics, service levels and management mechanisms shall be identified to guarantee the security of the network services provided by the suppliers.

6. Handling the media

.1 The use of extractable information media shall have the prior authorisation of Lantik and shall be for the exclusive purpose envisaged in the contract.

.2 At the end of the contractual relationship with Lantik, the extractable media facilitated to the supplier to implement its functions shall be returned.

.3 The use and storage of data on extractable media and the handling of the data shall comply with Lantik regulations.

.4 Access is forbidden to the Lantik documentation, located in both automated and non-automated repositories, unless express access has been given for the purpose described to provide the contracted service.

7 Data exchange

.1 Checks, procedures and techniques to protect the data exchange between the service provider and Lantik according to the critical nature considered by Lantik.

.2 Data exchange and its processing shall be governed by means of the relevant agreement or contract between Lantik and the supplier in question.

.3 When the service provision includes data transfer, the supplier shall implement technical and regulation checks that avoid the improper use or their deterioration. Lantik hereby reserves the right to audit those checks or require that additional protection is introduced.

.4 Lantik may require that the data transmitted by electronic messenger is adequately protected by the supplier, by means of requiring compliance of a specific regulation and/or the implementation of auditable technical controls.

.5 The transmission of Lantik data to other organisations is forbidden. When necessary to provide the contracted service, the service provider shall seek the authorisation of Lantik prior to transmitting the data in question. Depending on the classification levels and the established legal requirements, Lantik may request specific security checks that may be audited.

8 Monitoring

.1 Lantik shall set up the monitoring elements that enable the security events, exceptions and activities of the supplier to be audited according to the needs of the organisation. These records shall be kept for the time deemed to be necessary to act as evidence and/or supervise the access control.

.2 The use of the data systems shall be supervised by the supplier and this information shall be periodically processed.

.3 The operating and administration activities that may be carried out by the service provider on the Lantik data systems shall be logged.

10. Access Control

Objectives

- To prevent unauthorised access to the data and data systems.
- To secure the access of the supplier by means of authentication and authorisation techniques.
- To control security when connecting the Lantik network to other public or private networks.
- Log and review critical events and activities carried out by the supplier in the systems.
- To make the supplier aware of its responsibility regarding the use of passwords and hardware.
- To guarantee data security when using laptops and remote facilities.
- Acquiring, developing and maintaining the data systems

1. Lantik requirements for access control

.1 The supplier shall only have access to those network resources, applications and information that are necessary to carry out the work required for the contracted service. The access rights shall be the minimum possible to meet those needs. The access control rules shall be established on a "need to know" basis".

2. User access management

.1 Any supplier, prior to providing and completing the service in Lantik, shall register and deregister as a user using the formal user registration and deregistration process that grants and cancels access to the data systems.

.2 Lantik shall be notified as soon as possible of any changes to the service provision that involves changing the individuals involved in the supply process in order to perform the relevant user registrations and deregistration. Lantik hereby reserves the right to audit the allocations periodically.

3. User accountability

.1 The supplier shall undertake to use good security practices when selecting and using passwords for its information system, particularly in those cases where there are no automatic password quality policies in place.

.2 The supplier shall undertake to keep the work station free of papers and data media if they are not being used and to hide the information on the screen when not in front of it.

4. Network access control

.1 The supplier shall be provided with access to the network services required to supply the contracted service.

.2 The external connections of a supplier to the Lantik infrastructures requires prior authorisation. Auditable security checks will be required according to the risk analysis of the connection.

.3 Physical and software access to the configuration and diagnostic ports of the Lantik infrastructures is forbidden. Such access shall be logged when required to define the service.

.4 Based on the segregated network architecture, the connections shall be established according to the specific connectivity needs to provide the service. The configuration of routes or accesses without the prior authorisation of Lantik is forbidden.

5. Access control to the operating system

.1 Access to the operating systems from the user's hardware will require the start of an authorised session with the Lantik domain, when required by the service. Specific administration functions will need to be assigned for the servers and communications hardware. In the cases when so required by the service.

.2 All the users will have a unique user identifier for their personal and exclusive use.

.3 The use of applications and/or utilities that could invalidate the access and/or application controls and those not associated to the provision of the contracted service is explicitly forbidden.

.4 Connection time restrictions shall be used for data information systems where extraordinary risk levels are identified.

6. Access control to applications and data

.1 Access to the data shall be restricted on a need-to-know basis for the services contracted from each supplier.

11. Acquiring, developing and maintaining the data systems

Objectives

- To comply with the security checks in the life cycle of the information systems.
- To comply with the applicable standards and procedures during the life cycle of the applications and for the hardware on which they are used.
- To govern the use of confidential information.
- To guarantee the correct processing of the applications.
- To guarantee the correct use of the data in the different development, testing and production environments.
- To minimise the technical vulnerabilities.

1. Security requirements of the information systems

.1 Prior to the contracting and/or acquisition of new services, Lantik will conduct a prior analysis of the data security. When deemed necessary, specific requirements will be included in this area, along with functional requirements.

2. Correct processing of the applications

.1 Input data authorisation will be established in the developed applications in order to guarantee that they are correct and appropriate.

.2 Internal processing controls will be established for the developed applications. The controls will allow any modification to the data integrity, either on purpose or by error, to be detected.

.3 Security controls will be established to guarantee the communication mechanisms between processes, the authentication and integrity of the messages.

.4 Controls will be established to validate the output data from applications to guarantee that the information stored is correct and appropriate.

.5 The Development and Maintenance systematics for applications existing in Lantik (procedures, technical instructions and formats) will be applied.

3. Encryption controls

.1 Data encrypting will comply with the requirements established by Lantik pursuant to business and legal requirements. A high encryption algorithm with no known vulnerabilities or weaknesses will be used, along with an appropriate computer tool for the use of the algorithm and key.

.2 The encrypted key used by the supplier shall be protected against modification, loss and destruction. The authentication of the public keys used will be taken into account. The authentication process will be carried out by using public key certificates issued by a recognised certification authority that will have appropriate controls and procedures to provide the necessary degree of confidence.

4. Security of the system archives

.1 The Lantik procedures will be used to install and update software in the production environments.

.2 The use of real data will be avoided in the testing environment. In the case of resorting to that type of data, the supplier shall hold the relevant Lantik authorisation and shall guarantee the dissociation of that data prior to their use. In any event, the data used for testing shall be always protected and controlled.

.3 Access to the source code of the programs and to the related elements (designs, specifications, authorisation and verification plans) will be strictly controlled by Lantik to avoid involuntary changes or the introduction of unauthorised functions.

5. Security in the support and development processes

.1 Prior to the introduction of new systems or significant changes being made to the existing ones, the supplier shall follow the change management process established in Lantik.

.2 Situations that allow information leaks to occur shall be avoided. The supplier shall undertake to notify Lantik of those situations as soon as possible.

.3 The development by the supplier shall be supervised and controlled by Lantik based on the previously established requirements in the relevant contract.

6. Managing technical vulnerabilities

.1 The technical vulnerabilities identified in the data system shall not be exploited by the service provider. Lantik shall be duly notified as soon as possible.

12. Managing data security incidents

Objectives

- To establish weakness and event communication channels relating to data security.
- To manage security incidents.
- To discover any security incidents.

1. Notifying event and weak points of the data security

.1 The supplier is required to notify any security incidence that occurs in the provision of the service. This notification shall be made as soon as possible using the User Helpline (CAU). The available monitoring, alerts and vulnerabilities will also be used to detect data security incidents.

.2 Any weakness, regarding data security, shall be reported using the User Helpline (CAU). There is no attempt to check any suspected weakness.

2. Managing data security incidents and improvements

.1 All the security incidents shall be managed by Lantik and it may ask the supplier for its input to help to solve them.

.2 Based on the aforementioned management, data will be provided that can be used by the parties involved to analyse and learn lessons from the situation.

.3 The evidence gathered when managing a security incident may be requested by the competent judicial authority. It should therefore be duly stored and safeguarded.

13. Lantik continuity management

Objectives

- To establish the guidelines to be followed to guarantee the continuity of the business processes.
- To establish the guidelines to be followed to activate and deactivate the plan

1. Aspects of data security in the Lantik continuity management

.1 The contingency plans arising from the business continuity plan, which enables the operations to be maintained or restored and guarantees the availability of the information at the required level and time, may require the intervention of the service provider.

.2 The business continuity plan and the ensuing contingency plans will be tested and updated periodically to ensure their effectiveness. Measures will be taken to ensure that all the members of the recovery teams, along with any supplier affected, known their responsibilities.

14. Compliance

Objectives

- To comply with the legislation, regulations and contractual provisions in order to ensure that Lantik and/or the employees are not penalised, or are found civilly or criminally liable as a result of the breach.
- To guarantee that the supplier complies with the Lantik politics, standards and security procedures.
- To review the security of the Lantik supplier periodically in order to guarantee the appropriate application of the security policy, standards and procedures, on the technological platforms and the information systems to provide the service.
- To optimise the effectiveness of the process to audit the service provider.

1. Compliance of the legal requirements

.1 The supplier shall guarantee compliance of the regulations in relation to the use of the materials that may be covered by intellectual property rights.

.2 The supplier shall ensure that the Lantik assets are protected against different threats, during the time and in the manner established in the contract, based on business, statutory and legal requirements.

.3 The supplier shall guarantee compliance of the requirements established by the Spanish Personal Data Protection Act (LOPD) and the measures envisaged in the Royal Degree that enacts it. Furthermore, the supplier entrusted with the processing of Lantik files with personal data shall comply with the Lantik requirements as the owner of those files.

.4 These Data Security Regulations for Suppliers, along any ensuing regulations, are elements that prevent the improper use both of the data and the data processing resources.

2. Compliance of the technical and security standards ad policies

.1 The supplier shall ensure, within its sphere, compliance of the data security regulations. The result of the compliance reviews and the ensuing corrective actions shall be proof of managing data security in each sphere of responsibility, to be considered in the reviews of the provision.

.2 According to the contracted service and the needs of Lantik, technical compliance checks will be performed on the data processing resources, based on the Lantik regulations to manage data security.

3. Consideration regarding the auditing of the data systems

.1 Compliance audits shall be programmed in order to avoid risks to the Lantik assets and the services provided.

.2 Both the audit tools and the logs obtained in the process shall be kept in different environments to operating and development ones in order to avoid any hazard or improper use. If a supplier takes part or completely performs an audit, a prior risk assessment may be conducted and specific security controls set for the supplier.

15. Audit

When so requested by Lantik, compliance audits may be conducted on the indicated points, in order to establish the degree of compliance of the Data Security Regulations for suppliers and establish corrective actions where applicable.

16. Related documents

Internal Standard NCS-1/1 Security Policy Standard: Computer Code of Conduct for Suppliers

17. REVIEW LOG

Review	Date	Modifications
00	**24/03/11**	**Standard approved**
01	**21/09/18**	**The original document has been reviewed and adapted to equality regulatory legislation.**