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

Security standard: Computer Code of Conduct for Suppliers

Prepared and updated by: Security Department	Reviewed by: 00
	Effective date: 02/05/2011

1. PURPOSE	2. SCOPE
The Standard seeks to establish the Security policy that helps Lantik suppliers to use the computer infrastructure and resources made available by Lantik appropriately.	It is applicable to the computer infrastructures and resources used by the Lantik suppliers, which include the hardware, programs, servers, networks, etc....., and which enable the use of computer tools, access to other network (for example: Internet, Intranet, corporate network), the use of corporate services such as email, access to applications, etc.....

CONTENTS

Security standard: Computer Code of Conduct for Suppliers

Reviewed by: **00** | Effective date: **24/03/11**

1. INTRODUCTION

1.1. Lantik has computer infrastructures and resources that guarantee an efficient and rapid service. These work instruments include the hardware, programs, servers, networks, etc....., that enable the use of computer tools, access to other networks (for example: Internet, Intranet, corporate network), the use of corporate services such as email, access to applications, etc.....

1.2. Given the widespread use of those resources and the responsibilities assumed Lantik when serving their customers, there is therefore the need to establish clear standards that help the supplier to use those resources appropriately.

1.3. Definitions

Administrators: People that monitor and control the correct operating of a computer system.
Updates or patches: Improvements carried out to the programs to solve problems (security, performance….).
BFA: Bizkaiko Foru Aldundia – Bizkaia Provincial Council.
CAU: User Helpline.
Passwords or Security keys: They are "keys" that enable the users to access and use the computer resources and infrastructure that BFA makes available to carry out their tasks.
User account or "User-ID": It is the user identifier, which is used to enter a computer system.
Internet addresses: Address that identifies a computer online. When you refer to it, you usually refer to IP addresses.
Information: It includes not only what is stored, processed, represented and transmitted by the computer systems, but also what is written or in print, projected by visual means and, even, communicated verbally.
Mobile IT: It includes all those elements that are taken out of the premises of the organisations, such as laptops, external hard disks, Pen Drives, telephones, PDAs, etc.....
Infrastructure: Set of elements or services considered necessary for Lantik to operate.
Supplier: Individual or company, not in the workforce, that provides services to Lantik or its customers.
Resource: Any part or component of an IT system.
(Data) network: Set of interconnected computers or hardware that can exchange information
Internal network: Data network where the exchange is limited to the business/administrative environment.
Information system: Set of files, processing, programs, media and, where applicable, hardware used for data processing.
User: All the employees, whether substitute, temporary or permanent, working for LANTIK, along with any person that by virtue of any relation has access to the information or resources of Lantik or its customers

2. SPHERE OF APPLICATION

2.1. The standards included herein shall be applicable to all Lantik suppliers.

2.2. For the purposes of this Computer Code of Conduct, supplier will be taken to be any individual or company, which provides services to Lantik or its customers, along by any external person that by virtue of any relation has access to the data or resources of Lantik or its customers.

2.3. The Code of Conduct is likewise applicable for any communications using the Lantik network, or the instruments and systems that, where applicable, the organisation has made available to the suppliers.

2.4. Should Lantik introduce and make available new resources to the appliers, other than those envisaged herein, and until more specific regulations relating to them are provided, the contents of the Computer Code of Conduct shall be applicable to their use.

2.5. Please consult the CAU regarding any query or technical consultation that may arise in relation to the contents of this Code of Conduct.

3. REASONS AND OBJECTIVES

3.1. The guidelines contained in the present Code of Conduct have been drawn up given the need to establish clear rules that (i) guarantee an efficient and appropriate use of the work computer and technical instruments and systems that Lantik provides the suppliers, (ii) avoid certain practices consisting of their incorrect or inappropriate use and (iii) guarantee compliance by Lantik and the suppliers of the different legislation provisions that are applicable.

3.2. They likewise seek to make suppliers aware of computer security within and outside the Lantik premises. Therefore, the standards and rules of the Code must likewise be adopted should the supplier have access to the corporate network from computers located outside the Lantik premises.

3.3. This Code likewise seeks to make the Lantik suppliers aware of the need to use the computer resources correctly to guarantee the quality commitments and confidentiality assumed with third parties (administrations, customers, companies, etc.....) and with the other suppliers, given that Lantik has acquired a very important commitment level in this sense with respect to its information, that must be disclosed or made available to third parties.

3.4. The introduction of the new information technologies within our organisation exponentially increases the risks that can be generated as the result of any disclosure of information outside the Lantik environment. This aspect is fundamentally significant in a public and institutional environment such as the one at Lantik. Therefore, given the sensitive and confidential nature of the work performed, Lantik has systems to monitor and supervise the use by the suppliers of the computer and technical instruments within Lantik.

4. GENERAL GUIDELINES REGARDING THE USE OF COMPUTER RESOURCES

4.1. The guidelines set out herein seek to clearly and transparently specify the use to be made of the infrastructure and computer resources. Lantik is at the disposition of the suppliers to clarify any doubt that may arise with respect to their compliance

4.2. Lantik aims to comply with the contents of industrial or intellectual property laws. Suppliers must therefore check, prior to using and/or making available to Lantik, programs or information, whether they are protected by the industrial or intellectual property law and always cite the sources in the case that they use any information in any work document..

4.3. All the information relating to Lantik activities is considered to be confidential and suppliers therefore hereby undertake to use the information solely and exclusively in order to carry out the entrusted work. The supplier shall comply with all the functions and obligations regarding the use of the data system according to Lantik regulations and current legislation, particularly, the LOPD (Spanish Personal Data Protection Act.

4.4. Lantik may request the immediate return at any time of any type of media that may contain information that has been disclosed or has been created by the supplier.

4.5. Lantik may audit the own or other resources that support the contracted services at any time.

4.6. Suppliers shall maintain the supplied resources in a state of optimum use, by eliminating the information that they consider dispensable or without value, to improve the performance and quality of Lantik services and guarantee sufficient effectiveness.

Professional use

4.7. Lantik hands over all the resources that it makes available to suppliers on the basis that they are used for professional purposes.

4.8. All the connections that occur through the Lantik network (corporate, Internet, etc.....) will be used for professional purposes.

4.9. Any other use is forbidden.

End of the relationship with Lantik

4.10. Lantik provides suppliers with the appropriate computer systems to carry out its functions while the relationship with them is in force. From the end of the partnership with Lantik, the supplier may not access the computer and technical equipments and therefore the files stored therein.

4.11. Should the former supplier have certain resources or computer equipment (laptop, media, data, etc.....) in its possession, it shall have to return them prior to the end of their relationship.

4.12. Likewise, if a supplier ends its relationship with Lantik, it shall leave all the archives and document intact.

4.13. The confidentiality obligations shall exist even after the end of the relationship with Lantik.

5. RIGHT TO AUDIT AND CONTROL

5.1. Lantik hereby reserves the right to audit the computer systems and use the available resources to control the use that each supplier makes of the media and computer resources supplied, when deemed necessary to protect the interests of Lantik and of the users, or when it is convenient for specific security and service reasons.

5.2. The aforementioned audits shall be conducted according to the guidelines set by the Computer Control Committee and fully respect all legal guarantees.

6. ACCESS TO THE CORPORATE NETWORK

6.1. All the accounts of the suppliers must be defined by a password.

6.2. Lantik suppliers must comply with the approved security standards.

6.3. No supplier will use the Corporate Network to provide access to third parties or entities.

6.4. The Lantik suppliers must report all problems that may arise with respect to the use of the Network to the CAU.

6.5. This resource will be used for a professional purpose.

6.6. Any other use is forbidden.

7. USE OF THE HARDWARE

General principles

7.1. This resource will be used for a professional purpose.

7.2. Any other use is forbidden.

7.3. Access or entry by any means into the computer systems of other users is expressly forbidden using a login or password of another user, without express authorisation.

7.4. Any time that a supplier leaves its work station for any reason whatsoever, it shall block its system to avoid third parties having access to the resources and applications to which the legitimate supplier is authorised.

7.5. With respect to the audit and control by Lantik of the correct use of the resources and hardware by the suppliers, Clauses 5.1 and 5.2 herein shall be applicable.

8. USE OF THE PROGRAMS AND COMPUTER FILES (SOFTWARE)

General principles

8.1. In any event, the confidential data may not be sent by any means to third parties or organisations other than the recipient of the information, except when covered by the general standards applicable in Lantik.

8.2. The computer files and programs handed over to the Lantik suppliers are for professional use.

8.3. With regard to the audit and review of the use of the programs and computer files by suppliers, Clause 5.1 and 5.2 herein shall be applicable.

Software security

8.4. An anti virus programme shall be installed on all the equipment used to provide the service. However, as those anti-virus programs do not fully eliminate the risk of a computer virus being generated and spreading, the supplier shall be completely diligent when running files from unknown sources. In case of any doubt, the supplier should not execute the file or program and directly contact the CAU.

8.5. Under no circumstances may suppliers deactivate the anti-virus program installed on the hardware.

9. BROWSING ONLINE

General principles

9.1. Under no circumstances may suppliers access Internet sites with games, sexual contents or which are offensive or attack human decency or fundamental rights.

9.2. This resource shall be used for professional purposes.

9.3. Any other use is forbidden.

9.4. Lantik may control and audit the Internet connection data from the computers used by the suppliers to carry out their work, along with the specific contents of those connections, pursuant to what is established in Clause 5.1 and 5.2 in this Computer Conduct Code.

10. USE OF EMAIL

Professional email

10.1. This resource shall be used for professional purposes.

10.2. Any other use is forbidden.

10.3. The confidentiality required between Lantik and its customers or potential customers necessarily means the use of the most appropriate communication system in relation to the nature of the communication to be performed. Therefore, apart from guaranteeing compliance of the applicable regulations, appropriate use and security, the contents of the communication must be able to be audited and controlled by the Lantik technical services.

General principles applicable to professional email

10.4. In order to prevent information leaks and guarantee an efficient service, the unnecessary sending of email is to be avoided, by limiting the number of addressees to the strictly necessary.

10.5. The interception and/or unauthorised use of messages or email addresses of other users of the Lantik computer system are expressly forbidden.

10.6. Lantik suppliers shall reject any email message that does not come for reliable sources, as it could contain viruses or malware codes, SPAM, etc.....

10.7. Lantik suppliers shall avoid the unnecessary dissemination of the email address, mainly by not participating in message chains, however altruistic they may seem.

10.8. Suppliers that use email must comply with the standards and policies established to guarantee the confidentiality and integrity.

10.9. With respect to the audit and control by Lantik of the correct use of email by the suppliers, Clauses 5.1 and 5.2 herein shall be applicable.

11. NETWORK UNITS (STORAGE)

11.1. The network units at the disposal of Lantik suppliers are only for professional use.

11.2. Under no circumstances may the network units at the disposal of the suppliers be used to store personal and not professional data.

11.3. Any other use is forbidden.

11.4. Suppliers that use network units shall comply with the standards and policies established to guarantee the confidentiality and integrity in the exchange of information.

11.5. With respect to the audit and control by Lantik of the correct use of network units (storage) by the suppliers, Clauses 5.1 and 5.2 herein shall be applicable.

12. RESOURCES PROVIDED BY THE SUPPLIER

12.1. This section applies to the resources provided by the supplier to render the service.

12.2. The Lantik Security Department shall be notified prior to the implementation of any such resources.

12.3. The resources shall not be implemented until they have been approved by the Security Department. This implementation may suppose the introduction of the controls proposed by the Security Department.

13. COMPLIANCE

13.1. Suppliers shall be liable for complying with the applicable legislation, such as the LOPD, LPI, LSSI, etc.....

14. REQUIREMENT TO COMPLY WITH THE CODE OF CONDUCT

14.1. Finally, Lantik considers that suppliers should be reminded of the need of following the aforementioned guidelines faithfully, in order to safeguard the privacy of the customers and users, improving the quality and capacity of the communications network and improving security.

14.2. Therefore, should suppliers fail to comply with the guidelines contained herein, Lantik shall be forced to exercise the appropriate measures. This is all without prejudice to any labour, criminal or civil liabilities that the supplier in breach may have incurred.

14.3. Furthermore, Lantik may stop the service in the computer or network appliance where the supplier may have used the computer and technical resources provided by Lantik that does not comply with what is established herein.

15. EFFECTIVE DATE AND TERM

15.1. All Lantik suppliers shall study and comply with the contents of this Code of Conduct. Its contents shall come into force on the 2 May 2011 and shall be effective until it is not amended or replaced by another. Until the aforementioned date, there shall be a transition period to enable suppliers to progressively adapt their work dynamics to the contents of this Code..

15.2. Lantik shall provide each of the suppliers with a copy of the Code in order to ensure that they are aware of the contents.

15.3. The supplier shall be responsible for disseminating this Code in its organisation.

15.4. Furthermore, the current Code shall always be available to suppliers in the Lantik Extranet and any new versions shall be duly published.

16. RELATED DOCUMENTS

NCS-173 DATA SECURITY REGULATIONS FOR SUPPLIERS

17. REVIEW LOG

Review	Date	Amendments
00	24/03/11	Standard approved