NCS-1 / 1	Bizkaia lantik
Security Standard: Computer Code of Conduct for Suppliers	
Prepared and updated by: Security Department	Review: **05** Effective date: **02/05/11**

1. PURPOSE	2. SCOPE
The Standard seeks to establish the Security policy to ensure Lantik suppliers to appropriately use the computer infrastructure and resources made available by Lantik.	It is applicable to the computer infrastructure and resources used by Lantik suppliers and includes the hardware, programs, servers, networks, locations 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.

CONTENTS

3. INTRODUCTION

3.1. Lantik has computer infrastructures and resources that guarantee an efficient and rapid service. These work tools include the hardware, programs, servers, networks, locations 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.

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

3.3. Definitions

Administrators
Update
BFA - DFB
CAU
Passwords
User account or "User-ID"
Internet addresses
Supplier
Information
Mobile computing
Infrastructure
User Profile
Administrator Profile (Secondary)
(Data) network
Internal network
Information system
User

4. SPHERE OF APPLICATION

4.1. The standards included in this Code shall be applicable to all Lantik suppliers.

4.2. For the purposes of this Computer Code of Conduct, supplier will be taken to be any individual or company providing services to Lantik or its customers, as well as any external person that by virtue of any relationship has access to the data or resources of Lantik or its customers.

4.3. The Code of Conduct is likewise applicable to any communication using the Lantik network or the tools and systems that, as applicable, the organisation has made available to the suppliers.

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

4.5. The standards included in the following NSG 1/1 Security Standard: Computer Code of Conduct Annex shall also apply to the individuals who administer Lantik computer resources or infrastructures. Annex for Administrators, which will be circulated to the administrators by the Security Department.

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

5. REASONS AND OBJECTIVES

5.1. 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 tools and systems that Lantik provides to 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 legislative provisions that are applicable.

5.2. The Code likewise seeks to make the suppliers aware of computer security both in 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.

5.3. This Code seeks to make Lantik suppliers aware of the need to use the computer resources to guarantee the quality and confidentiality commitments that we assume with third parties (administrations, customers, companies, etc.) and with other suppliers, given that Lantik has acquired a high level of commitment in this regard with respect to their information that must not be disclosed or be available for third parties.

5.4. 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 that of Lantik. Therefore, given the sensitive and confidential nature of the work performed, Lantik has systems in place to monitor and supervise the use by the suppliers of the computer and technical instruments within Lantik.

6. GENERAL GUIDELINES REGARDING THE USE OF COMPUTER RESOURCES

6.1. 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 full disposal of its suppliers to clarify any doubt that may arise with respect to their compliance

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

6.3. **Any information relating to Lantik activities is considered to be confidential**, and suppliers must therefore undertake to use the information solely and exclusively in order to carry out the entrusted work. Suppliers shall comply with all the functions and obligations regarding the use of the information system according to Lantik regulations and current legislation, in particular, data protection legislation and in the ENS (National Security Framework).

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

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

6.6. Suppliers shall maintain the resources made available in an optimum state of 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

6.7. All the resources that Lantik makes available to its suppliers are handed over in order to be used for professional purposes.

6.8. Any connections through the Lantik network (corporate, Internet, etc.....) shall be for professional purposes.

6.9. Any other use is forbidden.

End of the relationship with Lantik

6.10. Lantik provides suppliers with the appropriate computer systems to carry out their functions while the relationship with those suppliers remains in force. Once they cease to work with Lantik, suppliers may not access the computer and technical equipment and consequently the files stored there.

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

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

6.13. The confidentiality obligations shall remain even after the end of the relationship with Lantik.

7. RIGHT TO AUDIT AND CONTROL

7.1. 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 deemed appropriate for specific security and service reasons.

8. ACCESS TO THE PREMISES

8.1. Any person accessing the Lantik premises shall comply with the applicable access rules.

8.2. Should access to the Lantik premises be necessary.

- An ID card will be provided and must be clearly visible at all times.
- At the end of the service or visit, the card must be returned to the security post located on the ground floor of the Lantik building.

9. ACCESS TO THE CORPORATE NETWORK

9.1. A password must be set up for all supplier accounts.

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

9.3. No supplier shall use the Corporate Network to provide access to third parties or entities.

9.4. Lantik suppliers must report any problems to the CAU that may arise with respect to the use of the Network.

9.5. This resource must only be used for professional purposes.

9.6. Any other use is forbidden.

10. USE OF THE HARDWARE

General principles

10.1. This resource must be used for professional purposes.

10.2. Any other use is forbidden.

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

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

10.5. With respect to the audit and control by Lantik of the correct use of the resources and hardware by the suppliers, Clauses 7.1 and 7.2 herein shall be applicable.

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

General principles

11.1. 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.

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

11.3. With regard to the audit and review of the use of the programs and computer files by the suppliers, Clause 7.1 and 7.2 herein shall be applicable.

Software security

11.4. An antivirus programme shall be installed on all the equipment used to provide the service. However, as those antivirus 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.

11.5. Under no circumstances may the suppliers deactivate the antivirus program installed on the hardware.

12. BROWSING ONLINE

General principles

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

12.2. This resource must only be used for professional purposes.

12.3. Any other use is forbidden.

12.4. 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 content of those connections, pursuant to what is established in Clause 7.1 and 7.2 in this Computer Conduct Code.

13. USE OF EMAIL

Professional email

13.1. Under no circumstances shall Lantik provide resources of this type of suppliers.

13.2. 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:

13.2.1. 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.

13.2.2. The sharing of information between Lantik and suppliers shall be performed securely (encrypted) for the information classified as confidential.

General principles applicable to professional email

13.3. 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.

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

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

13.6. Lantik suppliers shall avoid the unnecessary dissemination of email addresses, mainly by not taking part in message chain, regardless of how altruistic the purpose may seem.

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

13.8. With respect to the audit and control by Lantik of the correct use of email by the suppliers, Clauses 7.1 and 7.2 herein shall be applicable.

14. STORAGE (Network units, collaborative work points, etc.

14.1. The storage at the disposal of Lantik suppliers is for professional use.

14.2. Under no circumstances may the storage at the disposal of suppliers be used to store personal and not professional data.

14.3. Any other use is forbidden.

14.4. Suppliers that use those resources shall comply with the standards and policies established to guarantee the confidentiality and integrity in the exchange of information.

14.5. With respect to the audit and control by Lantik of the correct use of network units (storage) by the suppliers, Clauses 7.1 and 7.2 herein shall be applicable.

15. RESOURCES THAT CANNOT BE REQUESTED BY SUPPLIERS

15.1. There is a series of resources that cannot be accessed or requested by suppliers. These are:

15.1.1. Corporate email.

15.1.2. Intranet access.

15.1.3. VPN access.

15.2. If any of the resources in the above list are essential to provide the service, that will be treated as an exception and as follows:

15.2.1. The supplier must notify and have the approval of the Lantik service manager.

15.2.1.1. If approved, the request will be submitted to the Security Department for its approval.

15.2.1.2. The resource will not be granted without the authorisation of the Security Department. This implementation may suppose the introduction of the controls proposed by the Security Department.

16. RESOURCES PROVIDED BY THE SUPPLIER

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

16.2. Before being incorporated into the Lantik infrastructure, the supplier must:

16.2.1. Notify and have the approval of the Lantik service manager.

16.2.1.1. The latter will be sent to Technological Policies for their approval or rejection.

16.2.1.2. If approved, the approval of the Lantik Security Department is required.

16.2.1.3. 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.

COMPLIANCE

17.1. The suppliers are responsible for complying with the applicable legislation, such as data protection legislation, ENS, LPI, LSSI, etc.

18. REQUIREMENT TO COMPLY WITH THE CODE OF CONDUCT

18.1. Finally, Lantik considers that suppliers should be reminded of the need to follow 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.

18.2. 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.

18.3. 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.

19. EFFECTIVE DATE AND TERM

19.1. All Lantik suppliers shall study and comply with the content of this Code of Conduct. Its contents shall come into force on 02 May 2011 and shall be effective until it is amended or replaced by another.

19.2. Lantik has made a copy available for each of the suppliers at http://lantik.bizkaia.eus/ca_contratacion.asp.

19.2.1. The latest version will always be available at this address.

19.3. Suppliers shall be responsible for disseminating this Code in their organisation.

20. RELATED DOCUMENTS

NCS-1/2 Data Security Regulations for suppliers

NSG 1/1 Security Standard Annex: Computer Code of Conduct Annex for Administrator staff.

21. REVIEW LOG

Review	Date	Amendments
00	24/03/11	Standard approved
01	20/10/11	• The User and Administrator definitions have been reviewed in Section 3.3 and definitions have been added for the User Profile and Administrator Profile. • A point has been included in Section 4 *Scope of Application* to indicate that the standards included in *NSG 1/1 Security Standard Annex: Computer Code of Conduct will apply to individuals with the administrator profile. Annex for Administrators,* to be supplied by the Security Department.
02	10/05/13	• The locations have been added to the scope of the document. • The Access to the Premises section has been added. • The requirement to always have the ID card visible while on Lantik premises has been added. • The transitional period in Version 01 (Heading 18) has been eliminated.
03	29/11/16	• Compliance mainly of ENS has been added. • Minor amendments regarding the handing in of media as there is no any medium exchange. • The email policy has been amended to forbid corporate mail resources. • The procedure to incorporate RESOURCES PROVIDED BY THE SUPPLIER has been improved. • The need to provide a copy has been eliminated as the document will be available for suppliers at http://lantik.bizkaia.eus/ca_contratacion.asp • The "Network Units" heading has been changed to "Storage" to include new types of network, SharePoint, etc. data repositories. • A new heading "RESOURCES THAT CANNOT BE REQUESTED BY SUPPLIERS" has been introduced to include new Lantik security policies, such as no VPN, no Intranet, etc. An exception procedure has been included.
04	21/09/18	• The standard has been adapted to GDPR: the references of the LOPD (Spanish Personal Data Protection Act) and Section 17 has been reviewed. PERSONAL DATA PROTECTION • The document has been updated according to the new organisational structure and neutral language used.
05	05/06/20	• The point 7.2, refering to the Computer Control Committee has been deleted, since it has been agreed that it is not necessary.