Approved by the Government Council on 18/6/2018

INFORMATION SECURITY POLICY

1. INTRODUCTION

The Information Security Policy has been prepared in compliance with the requirements of Royal Decree 3/2010 of January 8, which regulates the National Security Framework (hereinafter ENS) in the field of Electronic Administration. Article 11 of this Decree establishes the obligation for Public Administrations to have a Security Policy and indicates the minimum requirements that must be met.

This Security Policy also follows the recommendations made in the CCN-STIC-805 security guide from the National Cryptologic Centre, a centre attached to the National Intelligence Centre

The purpose of the National Security Framework is to create the necessary conditions for the trustworthy use of electronic means, through measures to guarantee the security of systems, data, communications, and electronic services, which allow citizens and public administrations to exercise their rights and fulfil their duties through these means.

The University of Almeria makes use of ICT systems (Information and Communications Technologies) to achieve its institutional objectives. Consequently, these systems must be administered with diligence, taking appropriate measures to protect them against any accidental or deliberate damage that could affect the availability, integrity or confidentiality of the information processed or the services provided.

Therefore, the objective of information security is to guarantee the quality of the information and the continued provision of services, acting in a preventative way, supervising daily activity and reacting promptly to incidents.

ICT systems must be protected against rapidly evolving threats which can have the potential to affect the confidentiality, integrity, availability, intended use and value of the information and services. To defend against these threats, a strategy that adapts to changes in environmental conditions is required to guarantee the continuous provision of services.

This implies that the organisation and its personnel must apply the minimum-security measures required by Royal Decree 3/2010 (National Security Framework 'ENS'), in addition to continuously monitor levels of service provision, monitor and analyse reported vulnerabilities, and prepare an effective response to any incidents to ensure the continuity of the services provided.

The organization must ensure that ICT security is an integral part of each stage of the system's life cycle, from its inception to its withdrawal from service, through development or procurement decisions and operating activities.

Security requirements and funding needs must be identified and included at the planning stage, in the invitation to tender and in the tender documents for ICT projects.

The organisation must be prepared to prevent, detect, react and recover from incidents, according to Article 7 of the National Security Framework.

1.1. PREVENTION

The organisation must avoid, or at least prevent as far as possible, that information or services are harmed by security incidents. To achieve this, the minimum-security measures determined by the ENS must be implemented, as well as any additional control identified through evaluating threats and risks.

These controls, and the security roles and responsibilities of all personnel, must be clearly defined and documented. To ensure compliance with the policy, the organisation must:

- Authorise systems before they enter into operation.
- Regularly assess security, including assessing any configuration changes made on a routine basis.
- Request periodic third-party reviews in order to obtain independent assessments.

1.2. DETECTION

Since any incident can rapidly cause services to deteriorate, operations must be monitored continuously to detect anomalies in service provision levels and actions must be pursuant to Article 9 of the ENS.

Monitoring is especially relevant once lines of defence are established in accordance with Article 8 of the ENS. Detection, analysis and reporting mechanisms shall be created which regularly reach those responsible, and when there is a significant deviation from the parameters that have been pre-determined as normal.

1.3. RESPONSE

The organisation should:

- Establish mechanisms to respond effectively to security incidents.
- Designate a point of contact for communications regarding incidents detected within the institution or in other UAL-related organisations.
- Establish protocols for the exchange of information related to the incident. This includes communications, in both directions, with nationally recognised Emergency Response Teams (CERT): Iris-CERT, CCN-CERT...

1.4. RECOVERY

To guarantee the availability of critical services, the organisation must develop continuity plans for ICT systems as part of its overarching business continuity plan and recovery efforts plan.

2. MISSION

As reflected in its statutes, currently in force, the University of Almeria is an institution governed by public law, endowed with its own legal personality and assets, which corresponds to the public service of higher education through teaching, study and research, with full autonomy and in accordance with the Constitution and the law.

Closely linked to the fulfilment of this mission, the organisation wishes to stress the need for an ICT infrastructure that prioritises and encourages open use, focused on functionality, connectivity and user experience, as priority tasks to achieve strategic and institutional goals .

3. SCOPE

Due to the institution's mission, illustrated in point 2 of this document, the organisation shall not implement this security policy across the entire information system.

On this basis, the organisation shall apply this policy across the majority of the ICT systems that it manages centrally through the Information and Communications Technology Service, and specifically across all those systems that are involved with rights being exercised by electronic means, with the fulfilment of duties by electronic means and with access to information or administrative procedures.

In practical terms, this security policy applies to the following services and the ICT systems involved in them:

- **Institutional ERP[1] Systems:**
    - Academic Management
    - Financial Management
    - HR Management
    - Research Management
    - Quality Management
    - Site Management
    - Virtual Campus

- **Electronic Administration Systems:**
    - Electronic Administration
    - User Support

- **Virtual Teaching System**

3.1. Broadening the Scope

In addition, while appreciating that the following service is not directly within the scope outlined by the National Security Framework, it is agreed to extend the scope to the following UAL service due to its importance in the university community,**:**

- **Institutional Web System**

4. LEGISLATIVE FRAMEWORK

Spanish laws and regulations regarding the protection of personal data, intellectual property and the use of telematic tools are applicable. As a result, UAL may be required by the relevant administrative bodies to provide electronic records or any other information related to the use of information systems.

[1] ERP = Enterprise Resources Planning System. From the English *Enterprise Resource Planning*

This policy operates within the legal framework defined by the following laws and Royal Decrees :

- European Data Protection Regulation 2016/679, of the European Parliament and of the Council, of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and the free circulation of such, and repealing Directive 95/46/EC.
- Organic Law on Universities (6/2001) and modified by the Organic Law on Universities (4/2007).
- Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations.
- Law 40/2015 of 1 October on the Legal Regime of the Public Sector.
- National Security Framework (RD 3/2010).
- Organic Law on the Protection of Personal Data (15/1999) and its implementing regulation of Organic Law (RD 1720/2007).
- Law on Information Society Services (of 12 October 2002)

1. SECURITY ORGANISATION

1.1. DATA PROTECTION OFFICER (DPO)

This shall be a person with specialist knowledge in law and in the practice of data protection matters. This knowledge will be required in relation to the procedures that must be carried out, as well as the measures that must be adopted to guarantee that personal data which is subject to these procedures is correctly processed.

The Data Protection Officer must perform their roles and duties with complete independence.

The duties of the Officer as specified in Article 39 of the *GDPR*, are as follows:

- Inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to the GDPR and to other data protection provision.
- Monitor compliance with the GDPR, with other data protection provisions and with the policies of the controller or processor in relation to the protection of personal data , including the assigning responsibilities, awareness-raising and training staff involved in processing operations, and related audits.
- Provide advice where requested about the data protection impact assessment and monitor its performance in line with Article 35 of the GDPR.
- Cooperate with the supervisory authority.
- Act as the contact point for the supervisory authority on issues relating to processing data, including prior consultation of Article 36 of the GDPR and to consult, as appropriate, on any other matters.

1.2. COMMITTEES: ROLES AND RESPONSIBILITIES

The duties of the **ENS's Management Committee** are assumed by the current **Information Security and Data Protection Commission**, hereinafter known as the Security Commission.

The Security Commission shall keep the Governing Team informed.

The duties of the Security Commission in relation to the ENS are:

- Disseminate the Organisation's security policy and regulations.
- Approve the Organisation's security regulations.
- Annually review the security policy.
- Develop the procedure to allocate duties.
- Identify roles and responsibilities.
- Oversee and approve the National Security Framework's monitoring tasks:
  - Adaptations
  - Risk Analysis
  - Biennial Audit

1.3. ROLES: DUTIES AND RESPONSIBILITIES

Information owner

The **General Secretariat** shall have the role of information owner for the Organisation. The duties are as follows:

- Establish information security requirements.
- Work in collaboration with the security officer and the information officer to maintain the categorisation systems according to Annex I of the National Security Framework.

ICT services manager

The Managing Director will have the role as the Organisation's ICT services manager. The duties are as follows:

- Establish ICT services security requirements.
- Work in collaboration with the security officer and the information officer to maintain the categorisation systems according to Annex I of the National Security Framework.

Security Officer

The Manager of the Information and Communications Technology Service will have the role as the Organisation's security officer. The duties are as follows:

- Maintain the security of information handled and services provided by ICT systems with their scope of responsibility.
- Promote training and awareness of the Information and Communications Technology Service within their scope of responsibility.
- Verify that the security measures put in place are adequate to protect information handled and services provided.
- Review, finalise and approve all documentation related to system security.
- Monitor the security status of the system in place for security event management tools and audit mechanisms implemented in the system.
- Support and monitor investigations into security incidents, from notification to resolution.
- Prepare the periodic safety report for the system owner, including the most relevant incidents during the period.
- Approve the security procedures prepared by the information officer.
- Prepare the institution's security regulations.

This role of "Security Officer" described by the ENS, is not the same as the security officer role in UAL's documents.

IT Information Officers

The Service Managers of the Information and Communications Technology Service shall be appointed the role as the Organisation's Information Officers. Within their area of work, the duties are as follows:

- Develop, operate and maintain the System throughout its life cycle: its specifications and installation, and verify that it functions correctly .
- Define the Systems topology and management policy, establishing the criteria for its use and the services available in it.
- Define the connection or disconnection policy for equipment and new users in the System.
- Approve changes that affect the security of the System's operating mode.
- Decide on the security measures that the suppliers of System components will apply during the stages of its development, installation and testing.
- Implement and control the System's specific security measures and

make sure that they are properly integrated within the general security framework.

- Determine the authorised hardware and software configuration to be used in the System.
- Approve any substantial modification of the configuration of any element of the System.
- Carry out the mandatory process of risk management and analysis in the System.
- Determine the category of the system according to the procedure described in Annex I of the ENS and determine the security measures to be applied as described in Annex II of the ENS.
- Prepare and approve the System's security documentation.
- Define the responsibilities of each entity involved in the maintenance, operation, implementation and supervision of the System.
- *Ensure compliance with the obligations of the System Security Administrator (SSA).*
- Investigate the security incidents that affect the System and, in such an event, inform the Security Officer or other delegated person.
- Establish contingency and emergency plans, carrying out frequent training exercises so that staff become familiar with them.
- In addition, the information officer may agree to suspend the handling of certain information or the provision of a certain service if he is informed of serious security deficiencies that could affect established requirements being met. This decision must be agreed with those responsible for the information affected, the service affected and the security officer, before being executed.
- Prepare the security procedures necessary for the person who works in the system.

System Security Administrator

The ICT Network and Security Services Administrator will have the role of System Security Administrator. Their duties are as follows:

- Verify the approval of security operational procedures
- Ensure compliance with security controls
- Ensure that the approved procedures for managing the information system are applied
- Monitor hardware and software installations, their modifications and improvements to ensure that security is not compromised and that they always comply with the relevant authorisations
- Oversee the monitoring of the system's security status
- Inform the Security Officers and the Information Officers of any anomaly, compromise or vulnerability concerning security
- Collaborate in the investigation and resolution of security incidents, from detection to resolution.

1.4. SECURITY POLICY

It shall be the task of the Security Commission to annually revise this Information Security Policy and either propose it is reviewed or remain without changes. The Policy shall be approved by the Governing Council and disseminated so that all affected parties are aware of it.

2. PERSONAL DATA

The UAL processes information in which it uses personal data, adopting the appropriate security measures in line with the guidelines of the EU General Data Protection Regulation, the recommendations for the Data Protection Officer and maintains sufficient diligence to comply with the principle of proactive responsibility and the principle of accountability established by current security regulations.

3. RISK MANAGEMENT

All the systems subject to this Policy must perform a risk analysis, evaluating the threats and risks to which they are exposed. This analysis will be repeated:

- Regularly, at least once every two years
- When the information which is handled changes
- When the services which are provided change
- When a serious security incident occurs
- When serious vulnerabilities are reported

- When directed to do so by the Data Protection Officer

For standardising risk analysis, the Security Commission shall establish a benchmark for the different types of information which are handled and for the different services which are provided.

The ICT Security Committee shall streamline the availability of resources to meet the security needs of the different systems, promoting horizontal investments.

4. SECURITY POLICY DEVELOPMENT

This Policy will be developed through security regulations that address specific aspects. The security regulations shall be available to all the members of the organisation who need to be aware of them, in particular for those who use, operate or manage the information and communication systems.

The security regulations shall be available on the intranet, through the electronic administration portal (http://ae.ual.es), and the Security Commission's webpage (http://seguridad.ual.es)

Printed copies are also available in the Information and Communications Technology Service.

5. STAFF OBLIGATIONS

All UAL members are obliged to be aware of and comply with this Information Security Policy and the Security Regulations developed from it; it is the responsibility of the Security Commission to arrange the necessary means so that the information reaches all those affected.

All UAL employees shall attend an ICT security awareness event at least once every two years. An **action plan shall be established** for on-going awareness raising to be attended by all UAL members, particularly new members, while always taking into account UAL's budgetary resources.

Those who are responsible to use, operate or administer ICT systems shall receive training in the safe handling of systems to the extent they need it to carry out their work. Training will be mandatory before taking on any responsibility, regardless of if it's your first employment, a change in role, or a change of responsibilities within the same role.

6. THIRD PARTIES

When UAL provides services to other organisations or manages information from other organisations, they will be involved in this Information Security Policy. To this end, communication channels to report and coordinate with the respective Coordination

Committees of the ENS will be created and operating procedures will be established on how to react to security incidents.

When UAL uses third-party services or transfers information to third parties, they will be involved in this Security Policy and the Security Regulations that pertains to said services or information. Said third parties will be subject to the obligations established in the aforementioned regulations and may develop their own operating procedures to satisfy these regulations. Specific procedures to report and resolve incidents will be established. It must be ensured that third-party personnel are made adequately aware of security matters, at least to the same level as that established in this Policy. When some aspect of the Policy cannot be met by a third party, as required in the previous paragraphs, a report from the Security Officer will be required to specify the risks that are incurred and the way to deal with them.

The report must be approved by those responsible for the information and for the services affected before moving forward.

7. ENTRY INTO FORCE

This Information Security policy is effective from the day following its approval date by the UAL Governing Council and until it is replaced by a new Policy.

The previous Information Security Policy is repealed, which was approved by the University of Almeria's Governing Council on 17 December 2012.