Information Security Policy

Title	Information Security Policy
Purpose	Establish the information security policy of Uriach
Author	Cybersecurity office
Approved by	Risk & Compliance Committee

1. INTRODUCTION

The objective of this policy is to provide guidance and support for information security management, in accordance with business requirements and applicable regulations. To this end, the policy uses ISO 27001 as a reference framework, complemented by ISO 27002.

This policy contains a description of the key elements, such as human, organisational, technological and documentary, that Uriach applies to protect information and, especially, personal data, preventing the occurrence of security incidents that put them at risk.

At all levels of the organisation, the real and effective application of the measures set out in this policy will be ensured, so that this self-regulation system achieves the elimination of behaviours that could put the security of the information assets and personal data processed by Uriach at risk.

This policy shall be adapted to technological and legislative changes that may occur in the future, as well as to any organisational changes that may arise within Uriach.

2. SCOPE OF APPLICATION

Within the scope of application of this Protocol, we can distinguish the following:

a) **Corporate Scope -** This Protocol is applicable to all companies belonging to Uriach, as well as to subsidiaries and investee companies over which Uriach has effective control or holds a member position in the management bodies.
b) **Personal Scope -** This Protocol is applicable to all levels of Uriach, including management bodies, management positions, control bodies and all staff.
c) **Relational Scope -** The scope of application of this Protocol shall be extended, as far as possible, to suppliers, customers, subcontractors and employees.
d) **Geographical Scope -** This Protocol shall apply to Uriach's activities in any geographical area, whether local or international.

3. APPLICABLE LEGISLATION AND REFERENCE FRAMEWORKS

This policy is adapted to the following applicable regulations:

- EU General Data Protection Regulation (GDPR) 2016/679, of 27 April 2016, hereinafter also "GDPR".
- Organic Law 3/2018, of 5 December, on Personal Data Protection and guarantee of digital rights; and other applicable data protection legislation in Spain, hereinafter also "LOPDGDD".
- Data protection regulations in force in the countries in which Uriach or its subsidiaries carry out their activities.
- Regulations relating to the protection of critical infrastructures.
- National Security Framework (ENS) in relations with the Public Sector.
- Penal code.
- This policy uses the following reference frameworks:
- ISO/IEC 27001 Information Security Management Systems.
- ISO/IEC 27002 Code of practice for information security controls.

4. CONNECTION WITH COMPLIANCE

This policy is aligned with Uriach Compliance Model, in accordance with the following table of equivalences.

Regulatory structure	The most relevant information security policies, rules and procedures are listed in **ANNEX I** to this policy.
Control structure	The information security and data protection control structure are described in section 6.
Organisation chart	**ANNEX II** indicates the position of the data protection control bodies in Uriach's organisation chart.
Ethical Channel	Breaches of this policy and of the other rules and procedures in this area may be reported through Uriach's compliance channnel available in the intranet and Uriach's website.
Disciplinary system	Non-compliance will be sanctioned in accordance with Uriach disciplinary system.

5. OBJECTIVES AND PRINCIPLES OF INFORMATION SECURITY

Uriach's objectives in terms of information security are aligned with those of the business, giving priority to compliance with the legal obligations applicable to the activity it carries out.

Uriach's priority objective in terms of information security is to comply with the General Data Protection Regulation of the European Union and the regulations relating to the protection of personal and any other kind of technical regulation regarding confidential data in force in the countries in which it operates. For this reason, all levels of the organisation are committed to complying with the objectives set in terms of information security and the application of the established corporate controls.

Uriach's security strategy promotes compliance with the following fundamental principles:

- **Principle of confidentiality**: information must only be accessible to authorised users and may not be disclosed to third parties without authorisation.
- **Principle of integrity**: data shall be kept free from unauthorised modification and existing information shall not be altered by unauthorised persons or processes.
- **Principle of availability**: information shall be accessible and usable on an ongoing basis, ensuring process and business continuity.
    - This principle goes hand in hand with the principle of resilience: ensuring the resilience of systems and information after an incident that temporarily prevents access.
- **Principle of authenticity**: the origin and identities associated with the information are really those that appear in the attributes of the information.
    - This principle goes hand in hand with the principle of non-repudiation: ensuring that a user cannot deny authorship of an act in the system or the linkage to a piece of data or set of data.
- **Principle of traceability**: the possibility of always determining the identity of the persons accessing the information and the activity they carry out in relation to it, as well as the different states and routes the information has followed.
- **Principle of proportionality** between the controls to be applied and the seriousness of the risk to be prevented, detected or mitigated.

In new services and developments, the principle of security by design and by default shall be applied.

6. CONTROL BODIES, ROLES AND RESPONSIBILITIES

Uriach has differentiated the different roles and responsibilities in relation to compliance with the applicable regulations on personal data protection and information security. Likewise, all persons belonging to Uriach, whatever their position, are obliged to comply with the rules, procedures and controls established in the field of information security.

The control structure of Uriach is oriented towards the prevention of risks related to information security and, especially, to the prevention of infringements that may involve a violation of the fundamental rights of individuals in this regard. Thus, the control structure is based on the following scheme:

Board of Directors	The Board of Directors represents the highest level of the control structure. It may delegate control functions to such committees, departments and/or business areas and positions as it deems appropriate, with the sole exception of those powers that cannot be delegated by law.
Data Protection Committee	The Data Protection Committee is a collegiate body that, by delegation, assumes the functions attributed to the DPO, according to the GDPR. It is responsible for executing, approving and updating the Processing Register, as well as drawing up and analysing audit reports. The Data Protection Committee has a preventive function of the prevention model described in this policy and will have autonomous powers of initiative and control.
Risk & Compliance Committee	The Risk & Compliance Committee defines the compliance model of the entire organization and, among other issues, works in risk management in order to guarantee business continuity. The Risk & Compliance Committee interacts with the Board of Directors through the Delegated Compliance Commission.
DPO	The Data Protection Officer (DPO) assumes the function of representing the Data Protection Committee before the authorities, in addition to coordinating, accompanying and supporting the control officers of each department and/or business area, on whom the control function will fall.
Data Owner	A Data Owner has administrative control and has been officially designated as accountable for a specific information asset dataset.

Security Responsible	The Security Responsible is responsible for coordinating all Uriach's information security efforts.
Internal Audit	The Internal Audit Department is assigned the control functions set out in this policy and in its own regulations.
Executives Responsible for control functions	Both managers and managers responsible for control shall have their control functions assigned to them through the protocols, rules and procedures that affect them and, to the extent possible, in their Job Description (JD).
Employees with control functions	In some cases, control functions may be assigned to non-managerial employees. The assignment of these functions will be made through the protocols, rules and procedures that affect them and, to the extent possible, in their Job Description (JD).

Uriach shall adopt the necessary measures to ensure that staff are aware, in an understandable manner, of the data protection obligations that affect the performance of their duties, as well as the consequences of non-compliance.

7. CONTRACTUAL OBLIGATIONS

In addition to the legal requirements regarding security, Uriach is obliged to comply with the specific security requirements demanded by its customers and suppliers in relation to the information to which they may have access by virtue of their contractual relations with them.

In this sense, Uriach identifies and updates those contractual obligations that may be related to the security of the confidential information and personal data it accesses or processes. Likewise, Uriach shall periodically review and check that the contractual obligations assumed in information security are known at the appropriate levels within the organisation, and that their scope is provided for in this policy and in the rules and procedures that develop it.

8. INFORMATION SECURITY RISKS

Uriach's business activities include the manufacture, sale, distribution and marketing of healthcare and pharmaceutical products. Therefore, Uriach's main assets are intangible in nature and consist of confidential information, know-how, personal data, intellectual property and industrial property, among others.

The intangible nature of these assets makes them highly vulnerable to internal and external threats such as (i) unauthorised access, (ii) unauthorised copying, (iii) disclosure, (iv) transfer to third parties, (v) unauthorised use, (vi) unauthorised exploitation, and (vii) even destruction.

Likewise, the risks related to information security may acquire criminal criticality, as a technological crime. For this reason, Uriach establishes control measures aimed at mitigating, detecting and reacting to the commission of offences related to personal and family privacy, computer damage or the possible disclosure of company secrets.

Therefore, the protection of information assets requires the adoption of a series of legal, technical and organisational measures that are summarised in this policy and detailed in the different rules and procedures of Uriach.

In line with the above, Uriach periodically and continuously carries out an analysis of the risks and threats that affect information security.

The risk analysis (i) starts with the definition of an inherent risk map, through which the existing risk is evaluated before the application of prevention, detection and reaction controls, and (ii) generates a residual risk map, in which the net risks existing after the application of the controls are evaluated in an automated way.

Finally, there is an obligation at all levels of the organisation to immediately report any identified risks of non-compliance with personal data protection and information security regulations. These risks shall be communicated through the channels that Uriach has set up for communicating any type of risk of non-compliance, preferably: Uriach's compliance channel: Anonymous complaints channel / whistleblowing - URIACH (report2box.com) or dpo@uriach.com for any matter related to personal data infringement.

9. ASSET MANAGEMENT

Uriach periodically and continuously carries out an inventory of tangible and intangible assets to determine:

- Their economic value.
- Their level of vulnerability.
- Their importance for the business.
- The need to apply security measures to guarantee their protection.

The assets must have an identification code assigned to them, which may be the serial number in the case of physical assets and a unique name in the case of intangible assets; as well as identifying the servers, applications containing personal data, processes and laptops. In this regard, Uriach has a document for the delivery and return of corporate devices. In addition, all Uriach's information systems assets are identified in SAP.

10. INFORMATION CLASSIFICATION

Uriach promotes the following classification of information to know the level of confidentiality that must be applied to each document and to each type of data:

- **Confidential information**: non-public information of the organisation or personal data, the disclosure of which could cause damage to Uriach or to third parties. Confidential information may only be accessed, viewed and used by those persons expressly authorised and within the scope of the authorisation. The circle of authorised persons may temporarily include suppliers or customers where there is a clear justification or legal obligation to do so.
- **Information for internal use**: data that must not be reproduced or communicated outside the Uriach perimeter. This information may only be accessed, viewed and used by Uriach staff and in accordance with the permissions they have depending on their job position.
- **Public information**: there will be no restrictions on access, viewing or use.

Therefore, by default, all information that is within the Uriach perimeter and, especially, that which is in locked rooms or cabinets or in password-protected systems or applications will be considered confidential. A document or any data found within the Uriach perimeter does not need to be marked or stamped as confidential to be considered confidential.

As far as possible, confidential documents and data shall have a text, label, seal or attribute specifying the level of confidentiality or security that corresponds to it. Documents or data which do not have this characteristic shall also be considered confidential unless their public nature can be proven.

In case of doubt, the unclassified document or data shall be deemed to be confidential, and the relevant authorisation or clarification shall be requested regarding its level of classification.

11. PHYSICAL AND ENVIRONMENTAL SECURITY

Uriach assesses the risks and threats in the surrounding environment. This includes all sources of risk that could pose a risk to information security. Among others, the following are sources of risk:

- Critical infrastructures.
- Factories and companies with hazardous activities.
- Deposits of flammable materials.
- Deposits of explosive materials.
- High voltage lines.
- Radio frequency sources.
- Sentry boxes, cameras and fences.

If Uriach manages or is close to a critical infrastructure, it will consider the measures applicable in the regulations governing the prevention of risks associated with this type of infrastructure.

Likewise, if it is necessary and proportional, it is planned to contract an early warning service that includes warnings in relation to failures in the electricity grid or communications networks, changes in the anti-terrorist alert level, atmospheric phenomena, natural disasters and other threats that may put the safety of people and infrastructures of Uriach at risk.

12. PHYSICAL ACCESS CONTROL

Uriach controls the physical access of persons accessing its facilities, this being understood as the first level of the information security protection perimeter.

This control can be carried out directly, through its own technical and organisational measures on the facilities in which Uriach carries out its activity, or through a surveillance company specialised in physical access control.

On the other hand, the second level of physical access control is understood to be that of the areas, rooms or offices in which there are computer systems that house confidential information or personal data.

13. LOGICAL ACCESS CONTROL

Uriach controls the logical access of persons accessing the company's computer systems. The control of the logical access of persons to the company's IT systems is differentiated into different levels of protection:

- **First level**: it focuses on controlling access to servers, communications and any other channel that can be used for the input and output of information.
- **Second level**: desktop computers and terminals located in Uriach.
- **Third level**: corresponds to mobile devices: laptops, smartphones and tablets, among others.
- **Fourth level**: based on control over logical access to applications.

In line with the above, Uriach establishes and verifies that users only have authorised access to data and resources when they need it to carry out their functions for the organisation. Each server and each

application with confidential information or personal data manages the list of users and the profiles and permissions of each of them.

Likewise, the operating systems and applications used in the processing shall have mechanisms in place to prevent a user from accessing resources with rights other than those authorised.

Finally, accesses and failed accesses will be recorded in the corresponding log.

14. IDENTIFICATION AND AUTHENTICATION

Uriach adopts measures aimed at guaranteeing the correct identification and authentication of users. To this end, a system is established that allows the unequivocal identification of any user who tries to access Uriach ICT resources (PC, mobile phones, tablets, etc.) and the verification that he/she is authorised.

As far as possible, operations carried out on the corporate network or on the Uriach intranet are recorded in the log files of the servers. The use of the identifier and password assigned to each user will imply the acceptance, as proof of the operation carried out, of the records generated in said log files and stored in Uriach's computer system. Unless there is proof to the contrary, it will be presumed that the acts carried out with the assigned identifier and password have been carried out by the user who owns them.

15. USER MANAGEMENT

Uriach considers the types of users in the company, the people responsible for them and the functional manager of the information systems resources.

The type of users depends on if the user is an internal user or an external user. Those users have a responsible user with his/her responsibilities depending on the type of user they are responsible of.

Finally, there is a responsible user for accesses with the responsibilities of authorising the process of provisioning access to the resources, ensure the process of the cancellation of access to the resources, ensure the update of access levels to resources and periodically review of the resources under his/her responsibility.

16. PASSWORDS

Uriach considers the assignment, distribution and storage of passwords to guarantee their confidentiality and integrity.

The passwords assigned to each user of the corporate network are personal and non-transferable, and the user is solely responsible for the consequences that may arise from the misuse, disclosure or loss of the same. They must also follow the following criteria:

- The minimum length of the password shall be 8 characters,
- The password shall have a minimum of one upper case letter, one lower case letter, one number and special characters,
- The password shall have an expiry date of 90 days,
- None of the last 32 passwords used may be reused.

The user may not communicate or share the user ID and password with any other person. Unless there is evidence to the contrary, it shall be presumed that the activity carried out with said user ID and password has been carried out by the employee who holds them, and the latter shall assume any labour, civil or criminal liability that may arise from their use.

17. WORKPLACE SAFETY

Security at the workstation is regulated in the Rules for the use of Uriach's ICT resources. Each computer has a password-protected screen saver, which will be activated after a maximum of 5 minutes of inactivity.

Users shall apply a clean desk policy based on the digitalisation of their activity and the elimination of paper. Thus, documents to be used in paper format shall be kept in a locked cabinet at the end of the working day.

18. APPLICATION SECURITY

Uriach maintains and updates a list of approved applications, and no other application that is not on this list may be installed or used. The process of approving an application considers:

- The security of the application and the risks it may generate for the company, its users and third parties.
- The knowledge and reliability of the source or supplier of the application, so that an application that comes from unknown or unidentified sources or that does not offer guarantees of quality, security and reliability cannot be approved, installed or used.

Uriach shall keep a register of the applications used in each department. This register will describe the security measures established in each application, which will be verified with the corresponding checklist and with the information provided by the supplier. Likewise, when initiating the development of a new application, or the selection of one that already exists on the market, the characteristics it offers in terms of information security shall be assessed and considered.

Users will not have administrator rights over the corporate computers they use, so they will not be able to install applications without authorisation from Uriach.

Uriach plans to implement the necessary technological tools to configure URL filters, proxy servers and other network systems and utilities to prevent the downloading and installation of unauthorised applications.

There will be a test environment to install and test the main business applications before moving them to production. Testing prior to the implementation or modification of an application processing personal data shall not be performed on real data, but on fictitious data, unless the level of security corresponding to the processing is ensured. If testing with real data is planned, a backup copy must have been made beforehand.

19. SECURE SYSTEM CONFIGURATION

Uriach has and keeps up to date a protocol defining the appropriate configurations for Uriach security systems to be secure.

20. EXCEPTION MANAGEMENT

Uriach establishes security standards, but these are subject to changes or exceptions that must be applied to systems or assets owned by the organisation. Uriach considers and manages these exceptions and shall has an inventory of common exceptions already approved.

21. CHANGE AND CAPACITY MANAGEMENT

Uriach has a protocol that establishes the general guidelines that guarantee adequate control of changes in systems and services, and a correct integration of security in the processes of acquiring

systems and services. The aim is to reduce the risk of failures and guarantee availability. In addition to establishing the general guidelines to be considered in the planning of the capacity and performance of the systems.

22. PATCH MANAGEMENT

Uriach has a protocol that provides guidelines for the patching of vulnerabilities, so that systems can be adequately protected, ensuring their security and operation.

23. TEMPORARY FILES

For the purposes of this policy, temporary files are work files created by users or processes that are necessary for occasional processing or as an intermediate step while processing.

Temporary files and copies of documents that have been created exclusively for the performance of temporary or ancillary work shall comply with the security level applicable to them. Any temporary file or working copy so created shall be erased or destroyed once it is no longer required for the purposes for which it was created:

- Temporary files created automatically by applications shall also be automatically deleted by the applications themselves at the end of the session.
- Temporary files generated by operating systems shall be deleted periodically because of the automatic processes of the operating systems themselves, depending on their configuration, or manually, when necessary.

24. USE OF LICENSED SOFTWARE

Uriach will only use software that has been licensed for use. The use of unlicensed software is considered a threat to security, as well as an infringement of intellectual property.

Once a year, a software inventory will be carried out to determine the operating systems, utilities and applications installed on each Uriach server, desktop, laptop and mobile device.

The inventory will be compared with the list of licences contracted by Uriach. So that, if the number of licences is insufficient, the convenience of uninstalling the software not covered by the licences or acquiring the missing licences will be analysed.

25. VIRUSES AND MALWARE

Uriach establishes security measures to prevent the entry of viruses, malware and other similar threats into corporate systems. To this end, anti-virus, anti-malware and similar programs are installed and the corresponding update services are contracted.

Likewise, users receive adequate training and warnings to know how to identify, prevent and avoid the entry of viruses and malware through misleading messages and social engineering techniques.

26. COMMUNICATIONS SECURITY

Uriach keeps a register of the communications networks used, such as Internet. This register describes the security measures established in each network, which are subject to periodic checks.

In addition, when it comes to selecting a new communications provider, the characteristics offered by the same in terms of information security will be assessed and considered.

27. CYBERSECURITY MEASURES & AWARENESS

Uriach establishes cybersecurity measures that include protection against threats from communications networks, such as cyber-attacks, denial of service attacks, unauthorised access and system hijacking or ransomware, among others.

Likewise, Uriach establishes and keeps updated the appropriate security measures to avoid spam and the reception of messages that coincide with the phishing pattern. In this regard, the following is foreseen:

- **Providing training and awareness sessions** for the most at-risk staff to learn how to distinguish phishing and scams that use communications networks to achieve unauthorised actions such as money transfers and the hijacking of computers.
- **Sending reminder messages** about the most common deception or social engineering scenarios. For example:
    - Impersonating a manager to order an urgent and confidential transfer.
    - Impersonation of a supplier requesting a change of the current account to which invoice payments should be transferred.
    - Impersonation of a supplier to send false invoices with a different current account to pay them.

28. WIFI SECURITY AND WIRELESS NETWORKS

The Uriach Wi-Fi network, and any other corporate wireless network, has the necessary security measures to prevent unauthorised access and use.

Uriach establishes mechanisms to prevent users of corporate laptops and mobile devices, such as smartphones and tablets, from accessing Wi-Fi networks or any other type of wireless network that is not known and reliable.

Corporate laptops and mobile devices also have reinforced security measures, such as firewall and VPN, to prevent unauthorised access to the device or information through the communications networks that users use when they are outside Uriach. In addition, to access the internal network through VPN, multi-factor authentication (MFA) must be carried out.

29. MOBILE DEVICES

Uriach establishes appropriate security measures for corporate mobile devices and personal mobile devices authorised to have corporate applications installed (BYOD).

Users assigned corporate mobile devices must comply with specific rules of use and apply the corresponding security measures.

Users of BYOD devices must also comply with specific rules of use and apply corresponding security measures to ensure the security of corporate information that is stored on or accessed through the same device.

30. WORK AWAY FROM HOME AND TELEWORKING REGIME

Uriach endeavours to extend and reinforce the controls established in the field of information security to corporate or personal ICT resources used by users in their private homes.

The practice of teleworking must be approved by Uriach to ensure compliance with labour and information security regulations. The head of each department must approve the teleworking for his/her employees.

With the additional conditions to the employment contract, the criteria for how users are responsible and must treat confidential information and personal data are set.

In any case, the level of security corresponding to the type of data processed must be guaranteed.

31. CONTROL OF CRITICAL SUPPLIERS

Uriach keeps an updated list of all those suppliers who have direct or indirect access to personal data or confidential information. It includes all suppliers that may directly or indirectly compromise the security of information and are therefore considered by the organisation to be critical suppliers.

Special attention is paid to cloud computing and outsourcing service providers, especially when the type of outsourced functions is critical for the business or the provider assumes a strategic position that is vital for the organisation and for business continuity. Likewise, if it is necessary to contract a new service that requires access to data, Uriach will carry out a selection of suppliers and an evaluation and approval process that will consider the security measures necessary for the type of data to be processed, which will subsequently be detailed in the contract. The supplier selection and approval process will be based on the process that Uriach has developed in terms of compliance, adding the evaluation of the measures relating to information security.

In this evaluation, priority will be given to suppliers that have ISO 27001 certification or adhere to other standards in this area. This certification shall refer specifically to the type of services to be contracted and to the servers that will host the data.

The relationship with suppliers that have direct or indirect access to confidential information and personal data shall always be regulated in a contract that shall include (i) a specific section on information security measures, (ii) a regulation of the supplier's response times in a specific SLA for all matters related to information security.

Suppliers shall inform Uriach company with which they maintain the relationship of any type of subcontracting. Subcontractors are subject to the same requirements as the main supplier and must apply the same security measures.

32. MEDIA AND DOCUMENT MANAGEMENT

The supports and documents containing confidential information or personal data should identify the type of information they contain. Likewise, as an iniciatve, Uriach will make its best endeavours to make an inventory accessible only by authorised personnel of the documents containing information or personal data. When moving the media, measures must be taken to prevent theft, loss or improper access to the information during transport.

Whenever any document or medium containing confidential information or personal data is to be discarded, it must be destroyed or erased, by adopting measures aimed at preventing access to the information contained therein or its subsequent recovery.

The identification of supports containing confidential information or personal data that Uriach considers to be especially sensitive may be carried out using understandable and meaningful labelling systems that allow authorised users to identify their content and make identification difficult for other people.

There shall be a system for recording the entry of media that allows, directly or indirectly, to know the type of document or media, the date and time, the sender, the number of documents or media included in the shipment, the type of information they contain, the form of shipment and the person responsible for the reception, who shall be duly authorised.

There shall also be a system for recording the output of media which makes it possible, directly or indirectly, to know the type of document or media, the date and time, the addressee, the number of documents or media included in the dispatch, the type of information they contain, the form of dispatch and the person responsible for delivery, who shall be duly authorised.

The distribution of media containing confidential information or personal data shall be carried out by encrypting such data or using another mechanism that ensures that such information is not accessible or manipulated during transport or dispatch. Likewise, the data contained in portable devices shall be encrypted when they are outside the facilities under the control of Uriach.

The processing of personal data on portable devices that do not allow them to be encrypted must be avoided. If this is strictly necessary, reasons shall be given, and measures shall be adopted in accordance with the risks. Uriach, in any case, may limit the use of media to contain confidential information and personal data exclusively to those that have been approved, registered and authorised by the company.

33. BACKUP COPIES

Uriach periodically makes backup copies of the information to prevent its loss in the event of accidental or intentional destruction, guaranteeing its reconstruction in the state in which it was at the time of the loss or destruction.

The frequency, scope, place of conservation and restoration process of the backup copies is described in a specific procedure, and a supplier specialised in backup services may be contracted and audited.

34. CONTROL OF INCOMING AND OUTGOING INFORMATION CHANNELS

Uriach establishes controls to prevent the unauthorised entry and exit of its own and third party information. To this end, the channels of entry and exit of information, both digital and analogue, are identified, assessing the adoption, where appropriate, of controls.

Along these lines, Uriach regulates the process of selecting and hiring personnel to prevent the entry of confidential information and personal data from previous employment. Likewise, Uriach draws up and applies a protocol that regulates the process of voluntary resignation and dismissal to avoid the outflow of confidential information, both its own and that of third parties, and of personal data.

35. ANONYMISATION, PSEUDONYMISATION AND ENCRYPTION OF INFORMATION

As far as possible, and when necessary, Uriach will use irreversible or reversible dissociation techniques, based on the anonymisation or pseudonymisation of the data, as well as the encryption of the same, to protect the rights of the persons to whom they are associated and to ensure confidentiality.

- **Anonymisation** involves the irreversible removal of the fields that allow the identification of the natural person to whom the data refer, using additional procedures that avoid or minimise the risks of uniqueness, linkability and inference.
- **Pseudonymisation** consists of the reversible removal of the fields allowing the identification of the natural person to whom the data refer, and their replacement by an identifier that can only be associated to the data subject with a restricted access equivalence table.
- **Encryption** is based on a symmetric or asymmetric key system, provided that the key is strong and has the appropriate length and complexity, depending on the type of data to be hidden.

36. BUSINESS CONTINUITY

Uriach foresees the implementation of measures to ensure business continuity and the availability of corporate information and ICT resources. These measures may include, among others:

- An emergency plan with the actions to be taken if an incident of any nature prevents access to information.
- Alternative equipment, duplicate processing centres or suppliers with services or equipment that can replace the main equipment in the event of a breakdown or incident.
- A protocol for access to work documents of absent persons to ensure business continuity in the case of managers and employees who are absent from the company for a prolonged period due to travel, illness, breastfeeding leave or other similar situations.

Likewise, Uriach will implement the necessary measures to ensure that corporate ICT resources are constantly in proper working order and maintenance:

- In the case of software, all operating systems, applications, firmware and utilities, shall be updated with the latest versions, updates and security patches.
- In the case of hardware, Uriach will contract the necessary maintenance services and will have alternative equipment, duplicate processing centres or suppliers with services or equipment that can replace the main ones in the event of a breakdown or incident.

37. MONITORING OF ICT RESOURCES

Uriach has a system for monitoring the activity carried out in relation to corporate ICT resources and information assets. This monitoring is automatic and has, among others, the following objectives:

- The recording of activity for technical purposes.
- Ensuring the integrity of the information.
- Identification and prevention of possible attacks from external sources.
- Compliance with legal or contractual traceability obligations.
- Detection of equipment malfunctions.
- The compilation of statistics.
- Prevention of Uriach's criminal liability.
- The logging of activity for forensic readiness and evidentiary purposes.
- The logging of changes to the system.
- Ensuring the integrity of the information.
- The development of usage patterns.
- Issuing alerts on changes in usage patterns.
- Detection of non-compliance.
- Controlling the input and output of information.
- Ensuring business continuity.

Finally, in cases where the alerts issued by the system refer to possible misuse, non-compliance or offences, the corresponding investigation or inspection protocols will be applied.

38. DATA DESTRUCTION AND BLOCKING

Uriach has a protocol for the destruction of information that does not need to be retained or that has exceeded the established period for its retention. This protocol shall apply to the following material area:

- Tangible and intangible assets.
- Digital and analogue media.

- Confidential information, information for internal use and non-confidential information.

Finally, Uriach will also prevent access to the information by any unauthorised person, as well as the processing of blocked personal data.

39. VULNERABILITY MANAGEMENT

Uriach has a protocol that provides guidelines for reducing system risk through effective vulnerability management. To this end, a vulnerability management programme will be implemented which will include, among other things, pre-exploitation identification, risk assessment and risk remediation, to minimise the impact of cyber incidents.

40. SECURITY INCIDENTS

Uriach has a security incident management procedure that guarantees an immediate response to any threat to information security that may arise. Likewise, Annex III establishes a Security Incident Communication and Management Protocol, as well as the Security Incident Reporting Template to be completed by users and forwarded to the corresponding departments for the resolution of any incident.

Any person having knowledge or suspicion of any incident affecting information security must report it immediately through the channels established for this purpose. Failure to report a security incident will be considered a serious work-related offence.

41. REGULAR CHECKS

ANNEX IV details the main periodic controls that Uriach must carry out to verify compliance with this policy.

42. INFORMATION SECURITY AUDITING

If deemed appropriate, Uriach will undergo an information security audit aimed at assessing the risks contemplated in this policy. This audit may be internal, external or mixed, and shall include a verification of the existence, suitability and effectiveness of the security measures.

Such an audit shall be carried out on an extraordinary basis whenever substantial modifications are made to the corporate ICT resources that may have an impact on compliance with the security measures in place to verify the existence, suitability and effectiveness thereof.

The audit report must assess Uriach's compliance with external and internal regulations, identify its deficiencies and propose the necessary corrective or complementary measures. It must also include the data, facts, observations and evidence on which the conclusions reached and the recommendations proposed are based.

43. INTERNAL INVESTIGATIONS AND INSPECTIONS

Uriach may carry out an internal investigation or inspection of any of the corporate ICT resources.

- **Investigations** will have a wider scope of action than inspections and may involve several departments and/or business areas, processes or teams. They can be carried out at any time, preventively or following the communication of a risk.
- **Inspections** have a more limited scope of action and must be based on a reasonable suspicion of the existence of an offence or a breach of internal or external regulations.

44. TRAINING AND AWARENESS

Uriach will promote a constant training and awareness-raising activity at all levels of the organisation in the field of data protection and information security. This training activity will take the form of a Training Plan that may include both face-to-face sessions and e-Learning courses.

Awareness-raising may be based on any type of communication and training materials and tools to raise awareness of the risks of breaches at all levels of the organisation.

45. UPDATING AND IMPROVEMENT OF THIS POLICY

This policy is subject to continuous review and updating, to reflect the changes and improvements made in the field of data protection.

Likewise, Uriach, through its Data Protection Committee, constantly monitors the application of the prevention and control measures, and will propose, if necessary, the appropriate modifications under the following circumstances:

- When relevant breaches of this policy are brought to light.
- When significant changes occur in Uriach or in the activity it carries out.
- When changes occur in Uriach's information systems.

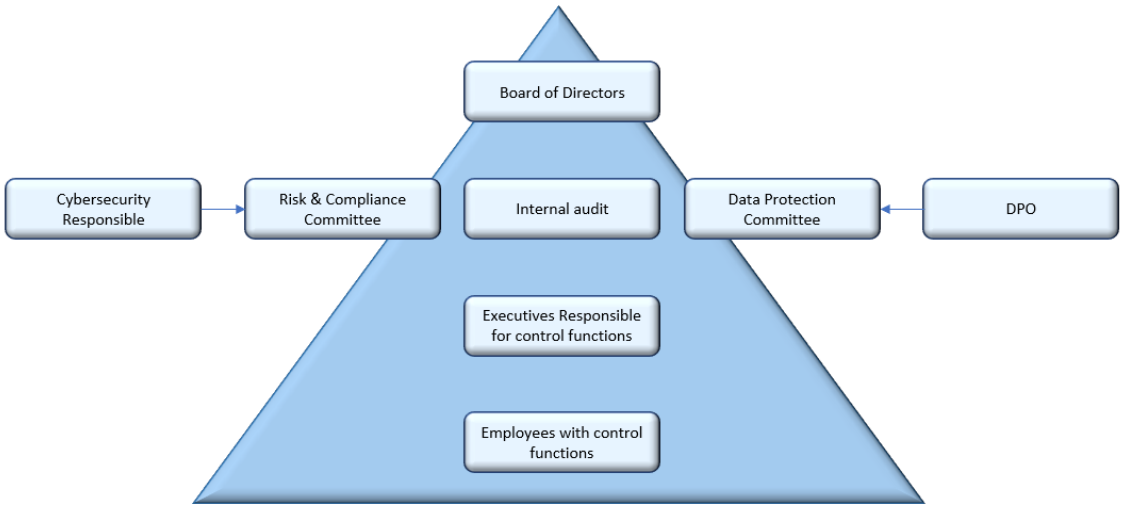
ANNEX I LIST OF THE MOST RELEVANT INFORMATION SECURITY POLICIES, STANDARDS AND PROCEDURES

Policy
Information Security Policy

Protocol
Asset management
Information classification
Supplier service delivery management
Security requirements for third party contracts
Risk management
Compliance with legal and contractual requirements
Vulnerability management
Security requirements of information systems
Removable device management
Physical security
Network and communications security
Backup and recovery
Access management
Use of cryptographic controls and electronic signature
User identification and authentication management
Security audits
User management
Secure system configuration
Exception management
Change and capacity management
Patch management
Transfer of information
Awareness and training
Endpoint security
Cloud security
Business continuity
Malware protection
Logs management and monitoring
Security incident management
Acceptable Use for Technological Assets

Procedures
Asset management
Vulnerability management
Backup and recovery
Access management
Patch management

ANNEX II LOCATION OF THE INFORMATION SECURITY CONTROL BODIES IN THE URIACH ORGANISATION CHART



ANNEX III SECURITY INCIDENT COMMUNICATION AND MANAGEMENT PROTOCOL

If a risk is detected at any level of Uriach, it will be reported and managed immediately following the protocol described below.

Detection	All levels of the organisation must be aware that Uriach has a zero-tolerance criterion in terms of security-related risks and must therefore pay attention to any risk situation that may be detected.
Communication	Once a risk situation has been detected, if it is related with data, it will be immediately reported to the Data Protection Committee through the channels established for this purpose: If the risk is related to regulatory non-compliance, it will be reported to the Risk & Compliance Committee through Uriach compliance channel available in the intranet and Uriach's website.
Registration	The Data Protection Committee shall register the communication. In no case shall a communication be left unattended.
Assessment	The Data Protection Committee will assess the category of the risk and will determine whether it is a possible breach of the Information Security Policy or a situation originating from causes beyond the control of Uriach and any of the people who form part of it.
Assessment of the risk to the fundamental rights of individuals	The Data Protection Committee will check whether there has been a risk to the fundamental rights and freedoms of a person or group of people.
Archive	If the risk is not serious and if there has been no risk to the fundamental rights and freedoms of a person or group of people, the file shall be closed, without prejudice to the proposals for improvement of the security measures or of the Security Policy that are deemed appropriate.
Notification to the Spanish Data Protection Agency (AEPD)	If a risk to fundamental rights and freedoms has occurred, Uriach shall notify the AEPD of the security incident without undue delay and, if possible, no later than 72 hours after becoming aware of it. If the notification to the supervisory authority does not take place within 72 hours, it shall be accompanied by an indication of the reasons for the delay. The content of the

	notification shall be as set out in Article 33 of the GDPR.
Notification to data subjects	Where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, Uriach shall notify the data subject without undue delay. The communication to the data subject shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in Article 33, section 3, letters b), c) and d). Before the communication is made, a check shall be made as to whether any of the exceptions provided for in Article 34.3 of the GDPR apply.
Assignment **Investigation** **Resolution**	In the event of a possible breach or any other situation of risk related to personal data, the Data Protection Committee and the Compliance Committee will take charge of the investigation, adopting the proposals for improvement or sanctions it deems appropriate, in accordance with the provisions of the Prevention and Control Policy.

CYBERSECURITY INCIDENT REPORTING TEMPLATE	
Affected website, app, server	
Type of incident	
Incident detection date	
Incident start date	
Incident end date	
Affected personal data	
Actions taken	

ANNEX IV PERIODIC CHECKS

Uriach plans annually (Action Plan) the periodic checks to be carried out. These checks shall include those listed below:

1 Control of the application of this policy

- Existence of the security policy in the possession of those responsible for its application.
- Level of awareness of security obligations by users.
- Level of compliance with security obligations by users.
- Detection of non-compliance.
- Need for corrective measures.
- Need for disciplinary measures.

2 Control of the identification and authentication system

- Level of updating of the list of authorised users.
- Level of updating and appropriateness of permissions granted.
- Correct functioning of the identification and authentication system.
- Periodic change of passwords.
- Encrypted storage of passwords.

3 Control of the access control system

- Proper functioning of access control systems.
- Intrusion testing.
- Checking the content of logs.
- Proper configuration of logs.
- Reliability of physical access controls
- Respect of access limitations according to the user's workstation or position.
- Security of telecommunications.

4 Control of compliance with confidentiality and secrecy rules

- Classification of documents.
- Respect for the level of confidentiality of each document.
- Control of document distribution channels.
- Level of awareness.
- Detection of non-compliance.
- Need for corrective measures.
- Need for disciplinary measures
- Verification of encryption standards in telecommunications.

5 Control of media management procedures

- Identification and labelling of media
- Inventory of media
- Secure storage of media
- Compliance with the procedure for authorising the disposal of media.
- Measures to be taken when media is to be discarded or reused.
- Operation of input and output registers.
- Application of security measures to media leaving the protected area.

6 Anti-virus and malware control

- Regular updating of anti-virus software.
- Review of anti-virus control automation.
- Compliance with anti-virus control obligations.

7 Control of compliance with intellectual property rules

- Review of each terminal by means of network or workstation audit programs.
- Inventory of licences for use.
- List of approved software.
- Correlation between existing licences and installed programs.
- Control of contents and databases.
- Need for corrective measures.
- Need for disciplinary measures.

8 Control of the backup procedure

- Level of compliance with the obligations relating to the making of backup copies.
- Level of compliance with the established frequency.
- Level of compliance with the obligations relating to the storage of copies.
- Level of compliance with the obligations relating to recovery tasks.

9 Control of the security incident management procedure

- Level of compliance with the obligation to report incidents internally.
- Level of compliance with the obligation to respond to incidents.
- Level of compliance with the obligation to record incidents.