RYANAIR

INFORMATION SECURITY POLICY

1. INTRODUCTION TO INFORMATION SECURITY POLICY

1.1. INTRODUCTION

This document defines the Information Security Policy for Ryanair.

Ryanair has a duty of care to protect personal and commercially sensitive information belonging to its staff, clients and service providers. In addition, Ryanair is required to protect staff and client financial and personal data in accordance with legislation, regulation and industry standards, including Card Scheme Operating Regulations, Payment Card Industry Data Security Standards (PCI DSS), SOX, GDPR among others. This policy aims to address all relevant legislative, regulatory and standards requirements, and is based on Industry Best Practice for Information Security and Data Protection.

1.2. SCOPE

The policies described in this Information Security Policy apply to networks, systems, processes, people and data (including commercial, employee and customer data) belonging to Ryanair or its clients.

Networks are considered all physical, virtual and cloud networks owned, managed or used by Ryanair. Systems include all hardware (e.g. servers, firewalls, etc.), devices (e.g. PCs, laptops and mobile devices) and software. Data assets include all physical media and electronic data formats.

1.3. ROLES & RESPONSIBILITIES

This policy is maintained by the Head of Information Security and owned by the Chief Technology Officer of Ryanair. Any conflicts with any other policy or processes must be notified to the document owner to be resolved. This policy is an evolving document that is subject to regular review (at least on an annual basis) and is updated to ensure that it remains current with Industry Best Practice.

All Ryanair personnel, including temporary or contract workers providing services to Ryanair that may impact the security of networks, systems or data belonging to Ryanair or its clients are obliged to operate in accordance with the policies defined in this Information Security Policy. Specific responsibilities are defined in each named policy, where applicable. Where no specific responsibilities are defined, policy statements apply to all persons defined above.

The communication of these policies, and provision of regular security awareness training will be provided by Ryanair, and the acknowledgment of all personnel is the responsibility of Department Leaders to enforce. All contractors and third parties will also formally be made aware of the appropriate policies before they begin working on behalf of Ryanair. The development and distribution of Security awareness training content and materials is the responsibility of the Head of Information Security. The distribution of this policy and collection of acknowledgments from all Ryanair employees during on-boarding and as part of the annual recertification is the responsibility of HR Department.

Compliance with this policy is mandatory. Failure to follow this policy may be considered as gross misconduct and will result in disciplinary action, up to and including summary dismissal. Further, serious offenders may be liable for prosecution under relevant legislation applicable to their jurisdiction.

Compliance with policies is primarily enforced through process and standards documents that are developed by each business unit defining how they perform day to day operations in accordance with these policies.

1.4. POLICY EXCEPTIONS

Even though these policies are mandatory, there may be extreme circumstances where they cannot be followed. Any exceptions to this policy, and related standards or processes must be approved in writing by the Z-Level Management for further details on policy exceptions see Exceptions Policy within this Policy.

1.5. REFERENCES

Policies within this Information Security Policy are based on and refer to the following key resources:

- ISO/IEC 27001 Information Security Management
- PCI Data Security Standards
- OWASP
- SANS Institute
- National Institute of Standards and Technology (NIST)
- Center for Internet Security (CIS)
- GDPR General Data Protection Regulation

2. INFORMATION SECURITY POLICY

2.1. INTRODUCTION

Information Security is the preservation of Confidentiality, Integrity and Availability of information.

- **Confidentiality** – ensuring that information is accessible only to those authorised to have access and to prevent unauthorised disclosure.
- **Integrity** – safeguarding the accuracy and completeness of information and information processing.
- **Availability** – ensuring that authorised users have access to information and associated assets when required.

This Information Security policy and supporting policies provide a set of controls for ensuring that data security is maintained at all time. Compliance with NIST 800-53 standard is monitored by Information Security Team.

2.2. PURPOSE

The purpose of this policy is to protect Ryanair's information assets and systems from all threats, whether internal or external, deliberate or accidental.

2.3. SCOPE

This policy applies to all employees including temporary and contract workers, third parties, and all sensitive and critical networks, systems, applications and devices used, operated and managed by Ryanair or by third parties on behalf of the Company.

Sensitive networks, systems, applications and devices are considered those that contain client or employee data, or that, if compromised would result in significant loss of confidential data.

Critical networks, systems, applications and devices are considered to be those that, in the event of failure or breakdown would prevent the Company from performing its core business without invoking Business Continuity and Disaster Recovery plans.

2.4. POLICY STATEMENTS

Ryanair's policy is to:

- Protect the information assets of Ryanair and our clients from unauthorised or accidental disclosure, modification, denial of access, corruption, infection, misuse, loss or destruction, through the use of logical, physical, procedural and personnel controls.
- Permit the access to, use of and sharing of information by authorised users only in accordance with best practices and legal and regulatory compliance requirements. In particular, all staff, information systems, contractors and suppliers shall comply with all applicable legal and regulatory requirements.
- Satisfy all security obligations required by regulation and legislation as applicable to all regions of operation.
- Use security risk management technique to determine the threats to information assets and adopt cost effective and practical solutions to reduce or remove the risks.
- Develop, maintain and operate secure information systems to provide excellent service to Ryanair and our clients.

- Prevent the infection and spread of computer viruses and other malicious software on all systems commonly affected by malware.
- Develop, test & maintain business continuity plans to remove or reduce the impact on the business to acceptable levels of any disaster that affects information systems, premises or personnel.
- Protect information systems from unauthorised changes by enforcing a strict change management process via the Change Advisory Board (CAB).
- Demonstrate commitment to the principles of this policy by including information security as a factor in the evaluation and procurement of new information systems.
- Promote awareness of information security amongst Ryanair staff and contractors as appropriate. This will be achieved through the establishment and communication of policies, procedures and guidelines and by specific training and awareness campaigns.
- Monitor and review the implementation of this policy and report regularly on compliance, including auditing access to information assets.

2.5. INFORMATION SECURITY CONTROLS

The controls required to protect information assets against threats or to ensure compliance may include physical controls, logical controls, training and awareness raising and additional policies to provide guidance and protection.

Supporting policies are defined below and can be found on Ryanair intranet:

Information Security Governance and Control Policy	**Data Security and Communication Policy**	**Physical Security Policy**
Network Security Policy	**Access Control Policy**	**Device Security and BYOD Policy**
Wireless Security Policy	**Change Management and Software Development Policy**	**Third Party Security Policy**
System Security Policy	**Vulnerability Management Policy**	**Security Incident Response Policy**
		Exceptions Policy
		Cloud Security Policy

In addition, this policy is supported by other policies and procedures as referred to through the policy.

This Information Security Policy and other relevant policies and procedures are created and maintained in accordance with Industry Best Practice, and applicable standards, regulations and legislation so that they are consistent, accessible and unambiguous.

3. INFORMATION SECURITY POLICY

3.1. END USER RESPONSIBILITIES

Department Leaders are responsible for:

- Implementing information security and supporting policies within their business areas;
- Ensuring that staff members complete onboarding and annual Information Security training;
- Ensuring that staff members and contractors are operating in accordance with those policies.

All staff (including temporary and contract staff) have an individual responsibility for:

- Adhering to the policies and procedures as defined in this policy;
- Completion of on-boarding and annual Information Security training;
- Protecting Ryanair equipment issued to them (e.g. laptops, mobile telephones) against unauthorised access and damage;
- Immediately reporting actual or suspected security incidents in accordance with the Security Incident Response Policy;
- Any person requiring a local administrator user shall submit a ticket which outlines the risks posed by the use of a privileged account as well as rules which shall be followed, in accordance with Ryanair's Information Security Policy. The ticket shall be approved by the Department Leader.

3.2. MEDIA MOVEMENT

- Confidential or internal data must not be sent to any external party without authorisation from a senior manager and the data owner, e.g. 2 separate people.
- All physical media and hardcopy data classified as Confidential that is sent to an external source must be sent via secure courier or other secure delivery method, as approved in advance by the data owner to ensure it is accurately tracked. All data sent externally must be logged and those records retained for a period of 12 months.
- All physical media including back up media must be sent via secure courier using a tracked service.
- Media inventories of all stored media and hardcopy data should be maintained and reviewed on an annual basis.
- Physical media and hardcopy data must be kept in secure storage locations and access should be controlled according to the principle of 'need to know'.

3.3. CLEAR DESK

- Ryanair operates a clear desk policy. Employees must remove and lock away any confidential or sensitive documents when away from their desk for any period of time and at the end of each workday. Home workers must ensure that clear desk principles are followed to protect data from unauthorised persons including family members.
- All staff are responsible for ensuring that their desk or work area is kept free from confidential or sensitive information when unattended.
- All written and printed client and company confidential and sensitive information must be secured in a locked filing or storage system when not in use.
- All written and printed output must be disposed of in confidential waste bins or shredded when no longer required.
- Documents must be collected from printers, copiers, and fax machines as soon as practical and never left overnight.

- Desks in public areas, such as building receptions and client meeting rooms, must be kept free from customer and company confidential and sensitive information at all times.
- When confidential information must be processed in a public area, it must be kept out of sight and reach of the public as far as is reasonably practical.
- All IT systems must be secured when not in use. If an IT system will be unattended for a short period, a password-protected screen lock must be activated. If an IT system will be unattended for an extended period, the system must be logged off.

3.4. DATA DISPOSAL

- All data must be securely disposed of when no longer required regardless of the format in which it is stored.
- An automated process must exist to permanently delete electronic data in accordance with defined retention periods. A quarterly process must be in place to confirm that all electronic data has been appropriately disposed of as retention periods are met.
- All physical and hardcopy data must be manually destroyed as soon as it has reached the end of its retention period. A quarterly process must be in place to confirm that all physical and hardcopy data has been appropriately disposed of as retention periods are met.
- Hardcopy materials must be crosscut shredded, incinerated or pulped so they cannot be reconstructed.
- Electronic data and physical media must be destroyed according to the following requirements as retention periods are met:
    - Data must be rendered unrecoverable when deleted e.g. through degaussing or electronically wiped using military grade secure deletion processes or the physical destruction of the media;
    - If secure wipe programs are used, industry accepted standards must be followed and documented to demonstrate that secure deletion processes have been followed;
    - All physical media and hardcopy data awaiting destruction must be held in lockable storage containers clearly marked 'To Be Shredded'. Access to these containers must be restricted.

3.5. EMAIL, COMMUNICATION AND INTERNET

Email facilities are provided to Ryanair employees for business use and employees must follow the policy guidelines defined below when using Ryanair email services:

- The Ryanair e-mail system is intended for business use only; misuse of the e-mail system or other violation of these policies shall be cause for revocation of privileges, and may be grounds for further disciplinary action, up to and including summary termination of employment.
- Ryanair reserves the right to access the e-mail account of any employee and to monitor and record messages to safeguard the legitimate commercial interests of the Company, such as determining compliance or violation of the firm's e-mail policies, ensuring quality control standards and monitoring contractual commitments.
- Creating and distributing e-mail may be equivalent to creating a legally binding document under law. In addition, e-mails may also need to be disclosed in formal legal proceedings so careful thought should always be given as to whether an e-mail should be sent at all and the precise words used. Any defamation to Ryanair' reputation through poor e-mail etiquette will result in disciplinary action being taken.
- Ryanair shall retain the copyright and all other property rights to the e-mail network and to messages sent/received over the network.
- The Company cannot guarantee the privacy of messages on the network given the need to monitor and record messages in order to protect its legitimate commercial interests.

- The Company may monitor any message for purposes including (but not limited to) network and system administration, security, verification of adherence to Company policy, and/or validation of Company-related business, at any time, if authorised by the HR.
- Company Confidential material, which includes cardholder data, must never be transferred outside the Company without authorisation. Any Confidential or sensitive material must be transmitted using a secure method of communication, e.g. emails should be encrypted using strong cryptography, physical media should be distributed using secure courier services and tracked.
- E-mails shall not be used to transmit copies of software or any copyrighted materials where Ryanair is not the copyright owner or otherwise licensed or authorised to do so], including (but not limited to) application programs, utilities, games, viruses, etc.
- It is prohibited to copy any Ryanair owned software and transmit it outside the Company, unless as part of a contractual deliverable.
- E-mail attachments received from an unknown source should not be downloaded unless the employee knows or is informed by the Head of Information Security or his team that the attachment has been virus-checked. If in doubt, employees should always consult the Head of Information Security for advice and guidance. Any confirmed viruses should be reported to the Chief Technology Officer by the Head of Information Security/Infrastructure and Operations Manager.
- To raise the awareness of email security, Information Security Team runs regular phishing simulation exercises where the users receive fake phishing emails and are tasked with completing phishing training in case they fail the test and click on the link/open the attached within the phishing email.
- The e-mail system is not to be used for the creation or distribution of any defamatory, obscene, racist, sexist content or any other content which is likely to be regarded as offensive. A serious breach of this rule is likely to be seen as gross misconduct.
- E-mail space must be managed by employees to ensure that mailbox size limits are not exceeded. Unwanted e-mails must be deleted, and any saved messages must be deleted when they are no longer required for business purposes.
- Unless otherwise specified, e-mail accounts shall be disabled by the IT department upon receipt of proper notification that an employee, consultant, or other account holder, has left the Company or no longer requires access to e-mail.
- Ryanair system users with Internet permissions are granted access to the Internet for business purposes. Employees must follow the policy guidelines defined below when using the Internet from Ryanair issued systems or for business purposes.
- Ryanair reserves the right to monitor the usage and content of all web pages accessed from the internal systems.
- Access to the Internet should be limited to business use only. A limited amount of personal use is permitted inside of work hours, with Department Leader's permission.
- The browsing of pornographic or other obscene sites will constitute gross misconduct.
- Ryanair reserves the right to monitor all downloads from the Internet to ensure appropriate use of the Internet systems is restricted to that necessary for legitimate business reasons.

3.6. PASSWORD MANAGEMENT

- Passwords shall remain confidential and are not to be shared, posted or divulged in any manner.
- Passwords of privileged accounts shall be stored in PasswordState and access to relevant passwords shall be granted based on the user's job role.
- Users shall be forced to change their password when they log in to the system for the first time.
- Password resets shall only be performed by the authorized system administrator. All users who request password resets remotely shall be validated either by an authorized system administrator or by an authorized tool for self-resetting passwords before user's password can be reset.
- Information systems shall enforce users to change their passwords at least every 90 days. This timing shall be configurable to allow for future changes.

Non-privileged users standard password requirements:

- Minimum password length at least 8 characters long;
- The new password shall not be the same as the previous 13 passwords;
- Users must change the password after 42 days;
- Password shall contain the four-criteria character groups (upper case, lower case, numeric character, special character);
- Account shall be automatically locked out after 3 invalid login attempts;
- Non-privileged users upgraded password requirements – upon manager's approval and completing the Passphrase Training, users have the possibility to use a different policy with the following requirements;
- Minimum password length at least 16 characters long;
- The new password shall not be the same as the previous 13 passwords;
- Users must change the password after 365 days;
- Account shall be automatically locked out after 5 invalid login attempts.

For privileged accounts, such as domain administrators, enterprise administrators, local administrators & service accounts passwords shall be at least 16 characters long.

3.7. PHYSICAL SECURITY

- Ryanair office areas shall be safeguarded through electronic access control installed at the entrance of each floor.
- Security Cameras are installed at the main entrance area & all elevator lobbies for monitoring.
- Workstations and laptops are located in areas that are not openly accessible to general public.
- There should be no visible sign indicating the location of communications room/data centre.
- Access to communications room/data centre is restricted to authorised Ryanair staff and third-party contract personnel only.
- The granting, modification, review or termination of a user's access to the Ryanair 's offices is done in accordance to established access authorisation process. A list of all authorized individuals is kept and reviewed regularly by Facilities Department/Site Manager to ensure that access is appropriate.
- Each employee/visitor must be issued an individual access card. Access cards must not be shared or loaned to others. Lost or stolen cards must be reported immediately. No tailgating is permitted.
- Communications room/data centre must be secured by access card readers to prevent unrestricted and unauthorized access.
- The entry to communications room/data centre at Ryanair Head Office in addition to access card, requires the user to enter the confidential PIN number.
- Access in and out of communications room/data centre by visitors (vendors, maintenance personnel etc.) must be controlled and tracked. Visitors' access shall be logged, and these logs will capture a) Name of the visitor, b) Company that the visitor is representing, c) Date and time of arrival, d) Reason for visit, e) Date and time of departure.
- Communications room/data centre are equipped with CCTV.
- All 3rd party IT contractors requiring access to Head Office communications room/data centre are subject to proper identification at the main entrance without which access will be strictly prohibited.
- All 3rd party IT contractors for Ryanair must sign-in at the reception area. They will be allowed to enter the premises only for specific authorized purposes.
- All 3rd party IT contractors will be assigned a security badge and the badge must be worn prominently by the contractor.

3.8. DEVICE SECURITY

- All users are responsible for the proper use of the Business Systems equipment they have been assigned and must comply with the Company's policies and all applicable laws.
- Ryanair business systems and equipment should not be used for the creation, communication or storage of any libellous or defamatory material or material that could bring the Company to disrepute.
- Ryanair business systems and equipment must not be used for any purpose that may be construed as threatening or constitutes personal harassment or bullying or which may constitute a criminal offence.
- Ryanair' office-based equipment and software must not be removed from the Company's premises without appropriate authorisation.
- Employees or other staff must not use Company business systems and equipment that they do not normally have authorised access to without specific authorisation from their department manager.
- Employees must not use Ryanair assets to run their own or other parties' businesses, unless specifically authorised to do so by the CEO.

BYOD - please refer to **Bring Your Own Device Policy_End User** for details.

3.9. THIRD PARTY SECURITY

- Ryanair must have a formal agreement in place with all service providers defining roles and responsibilities, including security and Data Protection obligations for all services to be provided. A right to audit should be included in all supplier agreements.
- Supplier due diligence must be conducted prior to engagement. Due diligence processes may include both onsite and offsite review and risk assessment of supplier facilities, systems, policies and processes (see Vendor Risk Management Process for details)
- Access to Ryanair systems for third parties must be authorised by the Change Advisory Board ("CAB").
- Infrastructure and Operations Team will maintain an access list for all third parties with access to Ryanair systems.
- Third party suppliers and vendors must be monitored when accessing the Ryanair information systems and network.
- Connected entities or third parties with user access to Ryanair systems are to be granted access to networks and systems when required for business purposes. Where full time access is required, formal justification for access must be documented and authorised by the Chief Technology Officer. Third parties operating on behalf of Ryanair must comply with all applicable policies defined in this Information Security Policy.
- Any third parties contracted by Ryanair are obliged to notify the Company of any subcontracting of tasks and services provided to Ryanair.
- Any third parties contracted by Ryanair are obliged to notify the Company of any suspected or actual security incidents that impact Ryanair data, system or network assets without undue delay.
- All service providers considered in scope of PCI DSS (i.e. those who store, process or transmit cardholder data on behalf of Ryanair, or could directly or indirectly access or impact the security of cardholder data or the cardholder data environment) must, in addition to the requirement above:
    - Acknowledge responsibility for any cardholder data stored, processed or transmitted on behalf of Ryanair, and/or responsibility for all in scope PCI DSS controls as applicable to services provided by the supplier as part of the supplier engagement agreement.
    - Formally confirm that they adhere with the PCI DSS standard, prior to engagement. Ryanair will not engage a non-compliant provider for any card data handling purposes, or to perform functions that may impact the security of the Ryanair cardholder data environment.
    - Provide evidence of their PCI DSS compliance status at least annually, and on request by Ryanair.

3.10. CLOUD SECURITY

- To ensure secure adoption and usage of cloud services, all cloud-based services, including Infrastructure as a Service, Platform as a Service and Software as a Service (e.g. external web application) must be approved by the Head of Information Security and Change Advisory Board prior to acquisition and deployment.
- Business Owner of the prospective cloud solution shall follow the guidelines included in the Third-Party Security Policy and Vendor Risk Management Process to log the vendor and allow Information Security, Data Protection (GDPR) and Anti-bribery and Anti-corruption due diligence.
- Only cloud providers which have been fully approved will be granted access to Ryanair environment/ network, if needed and additionally approved by the CTO.
- The payment of service invoices will be settled on the condition that due diligence checks have been successfully completed.

RYANAIR

v1.4