Group Information Security Policy.

November 2025

Policy Details

Group Policy Name:	Group Information Security Policy
Group Policy Owner:	Group Chief Information Officer
Group Policy Custodian:	Group IT Head of Governance, Risk & Compliance
Effective Date:	November 2025
Next Review Date:	October 2026
Policy Version Number:	v4.1
Internal or External Use:	External use only
Policy Level	2

1. Policy Statement

1.1. Who We Are

ZIGUP plc ('ZIGUP' 'We', 'Us' or 'Group') and each of its group undertakings exists to keep customers mobile. We are the leading supplier of integrated mobility solutions and automotive services to a wide range of businesses and customers.

1.2. Why This Policy Is Important to Us

Protecting our business from malicious and accidental harm is an essential responsibility we all share and requires the right balance in facilitating technical operations whilst enforcing guidelines and policies that ensure that protect information and IT systems, whilst working safely, securely, and responsibly.

This policy is designed to meet the control objectives set out in ISO27001, Cyber Essentials, and PCI DSS Regulations; annual reviews must take into consideration any updates to these standards or schemes as they may affect this policy.

This Group Information Security Policy forms part of ZIGUP's information risk management framework, the policy provides guidance and direction to help to reduce the risk of issues and to help us in meeting our legal obligations under the relevant data protection and privacy legislation general data protection regulations and other relevant laws. Cyber and information security is about ensuring that the Group implements a secure environment to protect the confidentiality, integrity, and availability of all our information, this policy is written to help the Group achieve this objective.

This Policy is a cornerstone of effective governance and risk management, as well as a driver of continual improvement in what we do, and how we do it.

1.3. Who This Policy Applies To

This Policy applies to all colleagues (UK & Ireland) where they are acting on behalf of ZIGUP, whether engaged on a permanent or temporary basis as an employee and in addition to any external contractors, agency workers or third parties.

1.4. Policy Breaches

We have zero tolerance for breaches of this Policy. Breaches must be reported immediately, or as soon as practicable to the Group Head of IT Governance, Risk & Compliance.

Any breaches of this Policy may be subject to appropriate disciplinary action as per ZIGUP disciplinary procedures, or for non-employees, such as contractors, the termination of contract.

1.5. Our Commitments

ZIGUP is committed to the protection of its information and technology assets from threats whether internal or external, deliberate, or accidental, such that:

- The reputation and good standing of the organisation is maintained.
- Confidentiality and security of sensitive information is maintained.
- Integrity of information can be relied upon.
- Information and systems are available when the business needs them.
- Relevant statutory, regulatory, and contractual obligations are met.

1.6. Keeping This Policy Up to Date

This Policy will be reviewed annually, or if the need for an ad hoc review is identified e.g., a change in legal or regulatory requirements, or, where we identify improvements in how we are delivering good outcomes for customers.

For further advice or guidance on the application of this Policy, contact the Group IT Head of Governance, Risk and Compliance.

2. Policy Requirements

For the purpose of this document, the following terms are used throughout, unless explicitly stated otherwise:

- Colleagues, Contingent workers, 3rd parties and customers are referred to as “Users”.
- Technology hardware, systems, applications and cloud services are collectively referred to as “Systems”.
- Information and data are collectively referred to as “Information”.

2.1. Individual Requirements

2.1.1. Requirements Applicable to All ZIGUP Colleagues

At a minimum, all ZIGUP Colleagues must:

- accept responsibility for maintaining the security of the Information they handle and the safety of the IT equipment (including Mobile devices) in their custody and/or systems entrusted to their care
- complete all mandatory Information Security Training annually
- read and comply with the Group Acceptable Usage Policy (AUP)
- protect information, particularly when displayed on screens or when using meeting rooms by complying with clear desk / clear screen requirements in the AUP
- adhere to the Group Risk Management Policy and any additional controls when using ZIGUP Information Assets and Technology Systems
- report all Information Security incidents they identify as soon as possible to their line manager and the Group IT Service Desk (or local equivalent)
- ensure they classify and label Information when it is created and/or used through employment of the Group classification levels
- ensure that ZIGUP Information is retained or destroyed in alignment with:
  - Group Information Classification & Handling Policy
  - Group and Business Data Retention Schedules (where published)
- only process ZIGUP information classified as Confidential or Restricted on approved Technology Systems, as advised by line management
- only use approved methods of communication internally or with customers and third parties (defined by business unit - e.g. email, Microsoft Teams, SMS)
- only use approved storage locations for ZIGUP information, whether on specialist applications (eg Ingenium, Proclaim) or on shared facilities (eg OneDrive, SharePoint, Microsoft Teams)
- only use Group IT approved and encrypted portable storage devices (eg thumb drives, USB storage) with management authorisation
- ensure they protect ZIGUP Information by using approved ways to authenticate to Technology Systems
- only use pre-approved software on ZIGUP equipment

All colleagues must ensure they comply with above as a minimum but also their local specific policies (where these exist) to protect ZIGUP data and IT systems. Where clarity is needed, please contact your line manager or the IT Service Desk for assistance.

Requirements in this section are clarified in the Group IT Acceptable Usage Policy, which is the document which should be read by colleagues under normal circumstances.

2.1.2. Requirements Applicable to All People Managers

At a minimum, all ZIGUP People Managers must ensure that their team(s):

- complete mandatory Information Security training
- comply with information protection requirements (eg clear desk/clear screen)
- are only provided with the access to Technology Systems that they need to carry out their roles and that the access is revoked when it is no longer required
- comply with the Group Information Classification & Handling Policy when processing and handling ZIGUP Information

2.1.3. Requirements Applicable to Technology Colleagues

At a minimum, all ZIGUP Group IT and Business IT Colleagues must ensure that they:

- read and comply with this Group Information Security Policy
- read and comply with Group IT Policy Framework documents applicable to their role

2.2. Inventories of Assets

The Head of each Business Unit (including Group Functions) must ensure that:

- an updated inventory of their Information Assets and Technology Systems is maintained in line with section 2.3.1 below
- this inventory must include all outsourced or 3rd party systems
- the inventory may be maintained by Group IT on the Business Unit's behalf

2.3. Information Classification and Handling

2.3.1. Information Classification

Senior Leaders in individual Businesses and Group functions, supported by the Group CIO and the ZIGUP plc Data Protection Officer, must ensure they classify their systems and data in line with the Group Information Classification & Handling Policy.

This classification will drive completion of the Business Impact Assessments. Assessment(s) must be completed at least once per calendar year, and never be more than 18 months old. BIAs must also be reviewed in accordance with the appropriate frequency for the classification of the system or when system changes are planned, whichever is sooner.

2.3.2. Information Handling

The Group CIO must ensure that:

- the confidentiality of ZIGUP Information is protected in line with the classification allocated in section 2.3.1 above
- this protection is delivered throughout the information lifecycle, to include creation, collection, management and destruction

2.4. Operations Security

The Group CIO must, on behalf of ZIGUP, ensure that all systems adhere to ZIGUP Policies and Security Standards. In particular:

- Hardening of systems against malicious or accidental alteration of operating parameters or information stored
- Availability of data through appropriate backup and recovery processes
- Logging and log monitoring/analysis to detect or investigate unexpected behaviour
- Protection of physical devices, including portable and mobile devices
- Protection of ZIGUP information at rest and in transit through appropriate application of cryptographic solutions

2.4.1. Access Controls

The Group CIO must ensure that:

- access management systems are in place which use the principles of least privilege
- access management systems are in place which enforce the principle of segregation of duties, either at the account or task level
- access to Information Assets and Business Systems are designed and managed commensurate with their ratings.

2.4.2. Network Security

The Group CIO must ensure that all networks which permit access to ZIGUP information are controlled, monitored and appropriately segregated.

2.4.3. Incident Management

The Group CIO must ensure they manage identified security events and incidents that affect the Confidentiality, Integrity, Availability and Resilience of Group Business Assets to prevent damage, restore services and prevent recurring incidents.

2.5. System Development & Maintenance

The Group CIO, on behalf of ZIGUP, must ensure that ZIGUP Information is protected throughout the system lifecycle and that any systems deployed within ZIGUP adhere to the principle of “Secure by Design”.

Adherence is demonstrated through ensuring that development methodologies and practice complies with ZIGUP Policies, in particular those pertaining to:

- Data Security
- Vulnerability Patching and Configuration (scope and scale)
- Security Testing (eg Code Quality Reviews, Penetration Testing)
- Application Security (eg defensive coding practices)

2.6. Supplier Relationships & Outsourcing (inc Cloud Security, 3rd Party Services)

The Group CIO, supported by senior management in individual Businesses and Group functions (including Group IT), must ensure that ZIGUP Information is protected when it is processed via 3rd party suppliers (including downstream suppliers), including outsourced and cloud-based service providers. Adherence is demonstrated through assuring that 3rd party suppliers comply with ZIGUP policies and standards.

3. Declaration

- The contents of this Policy have been consulted and considered with identified interested parties as identified by the Group Policy Owner.

- This a Level 2 Group policy. The content and commitments of this Policy have been approved by the Executive Committee on 23rd October 2025.

- The content and commitments of this Policy is hereby signed off by the Chief Information Officer on 30th October 2025.