Totalmobile Privacy and Security Overview

Totalmobile

Digital Workforce Management

Table of Contents

Introduction

Document Outline and Purpose

This document provides an overview of the Information Security Management System (ISMS) put into place by Totalmobile to ensure the confidentiality, integrity and availability of customer information we may process, store, transmit and access on behalf of our customers. It outlines how the ISMS is organised and managed as well as providing an overview of the core security controls put into place to safeguard customer information. It is noted that a fuller framework of security policies, processes and controls is in place.

Document Scope

The scope and applicability of this document is aligned to the current scope of Totalmobile's ISMS. This means that the organisational and security control features described relate firstly to the development, implementation, deployment and ongoing management and support of Totalmobile product solutions and are equally applicable to data handled on behalf of customers by Totalmobile (in this instance data handling may relate to the processing, storage, access, viewing, transmission and amendment of customer data as applicable and authorised within the context of services and support provided by Totalmobile). A second application of the described security controls, processes and policies considered to be in scope is in the case of a solution being hosted by Totalmobile on behalf of our customers. In such instances, the selection and application of security controls will extend to the provision, implementation and ongoing management of hosting services.

Governance and Compliance

Applicable Frameworks

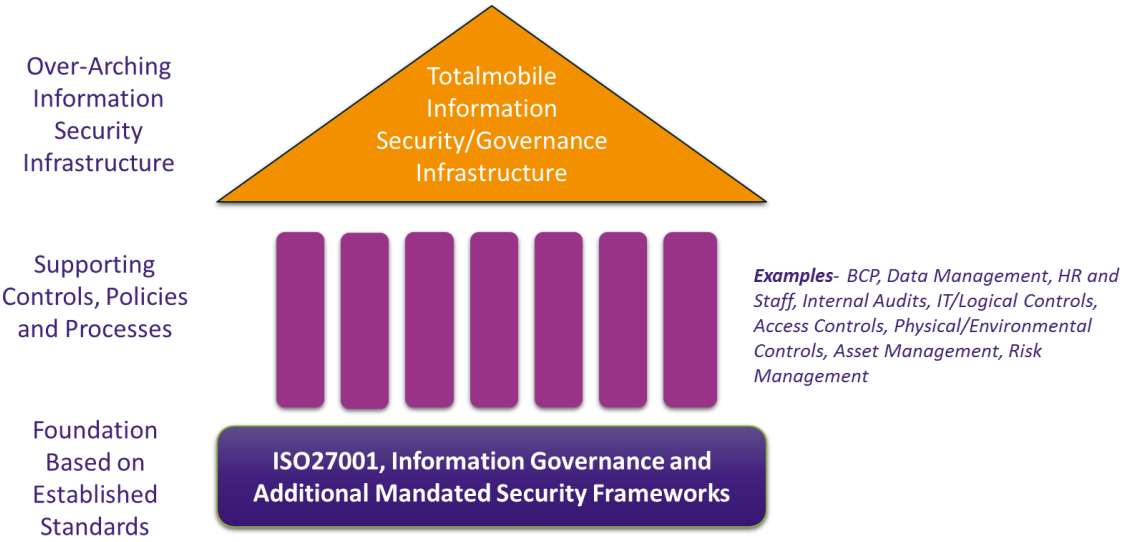
By adopting and implementing an Information Security Management System (ISMS), Totalmobile have committed to providing a robust security framework to ensure and safeguard the confidentiality, integrity and availability of both our own information, as well as that entrusted to us by our customers and partners.

Totalmobile's ISMS has been built in alignment to the ISO27001:2013 Standard, with principle security control selection and application being derived from this Standard. Totalmobile's ISMS has been certified as compliant to the ISO27001:2013 Standard since 2015.

In addition to the ISO27001:2013 Standard, Totalmobile have also incorporated additional governance and compliance frameworks into our overall ISMS to provide a more holistic approach to Information Security, governance and compliance. These frameworks include legal, regulatory and contractual obligations such as NHS Digital's Information Governance framework, applicable Data Protection legislation, the HMG Cyber Essentials framework and specific customer security requirements.

The Information Security Temple Model

To illustrate our approach to information security we have developed the 'Temple' model. This is outlined in the diagram below.



The 'Temple' is composed of three distinct elements; the base is comprised of the requirements prescribed by the ISO27001:2013 Standard, Information Governance frameworks and additional security controls mandated or required by our partners and customers, or in line with industry best practice. These form the 'Foundation' of our Information Security approach and provide an initial baseline against which our information security controls and efforts are aligned and ultimately assessed.

The pillars of the 'Temple' consist of the information security controls, policies and processes that enable the management of the ISMS. These control sets and frameworks are based on and supported by the various standards and requirements we adhere to and ultimately support the overall information security structure.

The roof of the 'Temple' model represents the overall information security infrastructure. This is the overarching information security infrastructure that represents the culmination of the supporting security controls and subsequent standards and information security standards and requirements. Within the model, the information security infrastructure embodies the overall information security protection for Totalmobile - forming a protective roof over the information and data held and maintained by Totalmobile, our partners and customers.

As a final point, the 'Temple' model also demonstrates our approach to information security; the supporting pillars (the controls, policies and processes) are given equal importance ensuring that there is no single point of failure within the overall information security infrastructure. Equally, the foundation of the entire infrastructure is based on established information security standards and governance, ensuring that there is a consistent reference point to the security controls implemented and maintained by Totalmobile. This baseline also provides the mechanisms to assess and audit the overall information security framework while equally enabling the opportunity to identify opportunities to improve and strengthen the ISMS.

Roles and Responsibilities

Dedicated staff resource and defined roles and responsibilities are in place to ensure the ongoing development, management and application of the principles and controls outlined within the ISMS and to ensure appropriate ownership of information security-related activities and risks.

Overall accountability for procedural documents and the implementation and management of the ISMS across the organisation lies with the Chief Executive Officer who has overall responsibility for establishing and maintaining an effective document management system, for meeting all statutory requirements and adhering to guidance issued in respect of procedural documents. Supplementary activities relating to information security are delegated as outlined below. A fuller outline of roles and responsibilities within the ISMS has been documented within Totalmobile's central Information Security policy.

- Chief Financial Officer (CFO):

  Totalmobile's CFO acts as the main Executive owner for the appropriate application and management of Information Security activities and compliance across the organisation. The CFO is also the Senior Information Risk Owner (SIRO) and provides an executive-level oversight on legislative, regulatory and contractual compliance, acting as a point of review and approval for applicable policies, processes and contractual agreements relating to information security.

- Head of Information Security and Compliance:

  Totalmobile's Head of Information Security and Compliance reports directly into the CFO, responsible for day-to-day compliance and governance activities, including ensuring adherence to required security frameworks and the management of the ISMS. Security management processes include the completion of asset and risk assessments and risk treatment, internal and external audits, incident management, identification of non-conformances and creation of corrective action plans, creation and maintenance of policy and processes, providing support, advice and guidance on security and compliance activities and leading information security training and awareness to all staff.

- Data Protection Officer

  The Data Protection Officer is the internal Data Protection lead and is point of contact for regulatory bodies and customers as well as for the escalation point for internal concerns.

- Information Asset Owners (IAOs):

  IAOs are typically departmental management or leads. Principally, they take ownership and responsibility for the assets and associated risks falling under the care or use of their department in conjunction with the Information Security Officer. They also take responsibility for fostering a culture that values information security, governance and compliance as it applies to their department, business activities and staff.

- Head of Technical Services:

  The Head of Technical Services takes responsibility for the formulation and implementation of IT related policies, and the creation of supporting procedures - ensuring that these are embedded within the development, implementation, management and review of robust IT security arrangements to meet identified risks and industry best practices. This includes the creation and testing of Disaster Recovery and Business Continuity processes. The Head of Technical Services also provides oversight and a liaison for hosted platform solutions.

- All Staff:

  As well as the above nominated positions, all staff are expected to understand, adhere to and apply information security policies and procedures as applicable to their overall organisational roles and responsibilities. This includes ensuring that they complete proscribed training and awareness modules and assessments, understand their role in compliance to contractual, legislative and regulatory requirements, as well as the responsibilities they have within processes such as incident reporting.

The PDCA Model and Continual Improvement

As the landscape of information security risk is continually evolving, Totalmobile adhere to the principles of the PDCA model to ensure continual monitoring and assessment of controls, policies and processes to ensure their ongoing applicability and suitability to provide an appropriately secure environment for the customer information we are entrusted with. The Plan, Do, Check, Act (PDCA) model has been incorporated into our ISMS to enable such monitoring and assessment to be carried out.

Control processes such as regular policy and process review, internal audits and quarterly asset and risk assessment are in place to objectively monitor adherence to defined security controls and processes, while also assessing their ongoing suitability and applicability to the context of providing security to our customers in the light of new technologies and emerging threat/vulnerability vectors. Sub-processes such as Incident Management, the identification of Non-Conformances and Risk Treatment are also in place to ensure that identified concerns and issues are appropriately controlled and resolved to prevent recurrence of the identified root cause of the said issue - such activities are regularly monitored, assigned a specific owner and actions assigned a specific timeline for resolution.

Both internal and external audits are also carried out on the ISMS as a whole to ensure that compliance to the ISO27001:2013 Standard is also maintained.

Risk Assessment, Control Selection and Application

Asset and Risk Assessment is a core element of the overall ISMS framework and forms the main engine of security control consideration, design and application. The process of risk identification is key in enabling Totalmobile to highlight threats and vulnerabilities to specific tangible and information assets. Our approach to risk management considers the value of an asset in terms of

confidentiality, availability and integrity and then calculates the potential impact and probability of loss or compromise of the asset. This provides a risk value which can then be examined against agreed risk appetite values and the perceived effectiveness of existing controls. This produces a residual risk score, which is then assessed against our risk appetite and acceptance criteria. It is this risk appetite that defines whether a risk response and mitigation is required; in cases where residual risk is identified as unacceptable a suitable response is devised by either the strengthening of existing controls or the implementation of additional controls where applicable. This is the Risk Treatment process.

Risk Assessment is carried out at regular intervals throughout the year, or in cases where a significant change is made to assets or data processing, or where prompted by the provision of a new service. The overall risk assessment process not only considers risk factors that impact Totalmobile, but also takes account of risks that may impact customers or arise from the provision of services to customers.

A review of residual risks, the effectiveness of existing controls, the application of new controls and progress towards closure of Risk Treatment plans is documented within quarterly reports as well as annually during the Information Security Management Review.

The selection, application and management of security controls are directly informed through the Risk Assessment process, derived from Annex A of the ISO27001:2013 Standard as well as applicable legal, regulatory and contractual requirements. Applicable security controls range from physical, logical and personnel controls in conjunction with defined processes and policy frameworks. Control application, alongside the justification for their selection and application, are documented within Totalmobile's Statement of Applicability.

Policy and Control Frameworks

Data Protection and Privacy

Totalmobile have incorporated compliance to Data Protection legislation within the body of the ISMS, meaning that logical, physical and policy/process controls are aligned to meet the requirements of safeguarding personal and personal sensitive information within our general security framework. In addition, with specific reference to processing data and information on behalf of customers, we adhere to the core principles of Data Protection and handle information only as requested within contractual agreements.

Specific policies around the handling, storage, access, visibility and transmission of personal and personal sensitive information are in place, which define how staff interact with such information as well as outlining the application of appropriate technical controls over such information. Training and awareness is provided to all staff with regards to these requirements and the application of controls with respect to the protection of personal and personal sensitive information is subject to regular auditing. Breaches involving personal or personal sensitive data will be notified to the ICO and investigated through Totalmobile's Incident Management process. In the case where such personal or personal sensitive data is being handled on behalf of a customer, then the customer will be advised, and support provided in fulfilling their own investigation processes and escalation to the applicable legal or regulatory body.

Cloud Services Security Overview

Data storage and processing is logically segregated among consumers of Azure or AWS and functionality specifically developed for multitenant services, which aims to ensure that consumer data stored in shared cloud service data centers is not accessible by another organisation. Fundamental to any shared cloud architecture is the isolation provided for each consumer to prevent one malicious or compromised consumer from affecting the service or data of another.

- Deployment. Each deployment is isolated from other deployments. Multiple VMs within a deployment are allowed to communicate with each other through private IP addresses.
- Virtual network. Multiple deployments (inside the same subscription) can be assigned to the same virtual network, and then allowed to communicate with each other through private IP addresses. Each virtual network is isolated from other virtual networks.
- Traffic between VMs always traverses through trusted packet filters.
- Protocols such as Address Resolution Protocol (ARP), Dynamic Host Configuration Protocol (DHCP), and other OSI Layer-2 traffic from a VM are controlled using rate-limiting and anti-spoofing protection.
- VMs cannot capture any traffic on the network that is not destined for them.
- Customer VMs cannot send traffic to cloud service private interfaces, or other customers' VMs, or cloud infrastructure services themselves. Customer VMs can only communicate with other VMs owned or controlled by the same customer and with Azure or AWS infrastructure service endpoints meant for public communications.

To verify isolation on the platform:

- Microsoft and AWS conduct ongoing penetration tests of the environment in accordance with the dynamic nature of the cloud to help ensure that a consumer's data remains private to them. Administrative functions are separated from other user groups, with permissions and privileges aligned specifically to each user role, where dual roles for a single user are required, for example System Administrator and System User, separate sets of login credentials shall be provided to prevent abuse of privilege.

SIEM is in place both for Totalmobile on an organisational level- firewall alerts, proactive network event and activity monitoring as well as within the cloud environment.

Internal Infrastructure, Network and Equipment Security

To provide a high level of safeguards and assurance on sensitive information held and accessed by Totalmobile, we employ numerous controls around the storage and transmission of data.

Principally, encryption is employed to protect data at rest and any data designated for transmission. Equally, all such data movement takes place via secured channels as governed by our Secure Transmission of Information policy.

In addition, mobile devices and workstations (including laptops) incorporate encryption within their standard build. No devices may be used to store or access sensitive or confidential information without this control being in place.

Dedicated firewalls are in place within Totalmobile's network infrastructure to protect against external threats and attack. This setup also incorporates intrusion detection and alerts to ensure that any attempted unauthorised access is detected, logged and assessed. Network infrastructures are also logically segregated.

As well as protecting against theft or interception, the corruption of data is mitigated through the deployment of backups (which combine both logical and physical controls) and dedicated AV facilities to protect against viruses, malware and ransomware-type attacks. Further detail on applicable backup processes is available in the Totalmobile Hosted Services Backup Policy. Additional Network Security and Acceptable Use Policies and associated controls are in place to define the appropriate use of Totalmobile equipment, network infrastructures, email and inter/intranet usage.

An additional control on Data Security lies within the provision of logical access to Totalmobile systems. Access to data is controlled on a least privilege basis and based on role and responsibility, with any additional access permissions needing to be formally requested, reviewed and approved prior to application to a user account. This applies to both internal Totalmobile staff and customers accessing our systems. Robust passwords are required to access Totalmobile networks; requirements for password strength, complexity and frequency of change are defined centrally and applied to all users.

Patching and vulnerabilities are proactively monitored and managed centrally by our Internal Services Team. Regular penetration testing is carried out to identify any potential vulnerabilities that have not been accounted for during regular monitoring, issues that are identified during such testing are assigned specific action plans to address.

Totalmobile Product Security Features

Totalmobile have designed and built our software with a robust set of controls to meet the expectations of our users and to provide assurance over the security of information processed through our application. Product offerings and solutions are periodically subjected to penetration testing.

Device Activation and System Administration

Before a user may use Totalmobile they must register their device and credentials. The user carries out an activation process on the device, which sends an activation request to the system administrator. The activation request includes both user and device identifying data. This process includes identity verification by the system administrator. The system administrator activates the device for the user, which provides authentication. System administration controls also enable devices and/or users to be deactivated, preventing access and use of the Totalmobile app.

User Authentication

Totalmobile authenticates a scenario rather than simply authenticating the user. This means that a combination of Unique Device Identifier (UDI), Username and Password must all be correct for a user to successfully authenticate to the app and access data. The impact of this is that even a valid user cannot log in from another user's device using their username and password. The correct user must log into the specific device that the administrator has activated them on.

This setup provides two factor authentication based on the principles of "Something the user has" (the particular device the user is registered with) and "Something the user knows" (their password).

Authentication details are exchanged each time a device communicates with the server during the use of the Totalmobile app. Credentials must be correct and the users account active for any data exchange to be successfully completed.

Edge of Network Authentication

Totalmobile does not require a network account for each user. This is important for organisations that are deploying mobile applications to users who would not previously have had access to the corporate network. This not only reduces the risk of a network being compromised, but also reduces the burden and complexity of system administration.

Secure Integration Model

The overall architecture of Totalmobile mitigates the risk of data falling into the wrong hands. Traditional models for remote access or mobile presentation of back office systems typically allow the user, once authenticated, to browse either the network or the actual back office system. In Totalmobile, the device receives only the data it is sent (based on a specific job or task) over an encrypted connection. At no time is the device provided access to back office systems or supplementary networks, therefore mitigating against the risk of unauthorised access into these back-office systems and the data residing within such systems.

Data Purging

Totalmobile further reduces the exposure to data loss by purging data from the device. Once transactions such as visits have been completed and processed, a server side archiving process will automatically remove them from the database and devices. The amount of work in progress carried at any given time at a device level is configurable and may be aligned to existing organisational standards, legal requirement or based on the nature or sensitivity of the data in question.

Operating System, Patch and Anti-Virus Compatibility

Totalmobile is designed to function with various operating systems and across multiple device platforms. We test the compatibility of Totalmobile with various operating systems, incorporating different versions and subsequent incremental patches, as part of our overall testing methodology. Furthermore, we have had no reported issues with Anti-Virus programs and Totalmobile does not enforce any kind of exclusion from Anti-Virus scanning, meaning Totalmobile does not negatively impact customer security controls.

Data Encryption

The Totalmobile app employs and applies robust encryption standards on both data at rest and data in transit, with information held or captured from the use of the app being logically segregated from other device storage, for example images captured through the device camera would be stored in a specific Totalmobile encrypted storage area and not on the device's central camera roll. The encryption is also localised to a specific device, meaning that information export or copying is not

possible, even to another device using the Totalmobile app. The way in which Totalmobile secures data precludes the requirement of a dedicated mobile device management software to enable secure deployment and use, however, Totalmobile is expected and designed to work with such software where it is already in use by an organisation.

App Lock when Backgrounded

The Totalmobile app may be configured to lock out immediately after it has been backgrounded and also enables subsequent configuration on how long the app may be backgrounded before it locks out. This forces users to re-enter their login credentials when returning to the Totalmobile app and mitigates the risk of data leakage caused by the app being left unlocked.

Password Management

It is possible to enforce password expiration onto instances of the Totalmobile app, meaning that a user's password must be changed after a given period of time. This provides a degree of logical access control to the app while also enabling instances of the app to be aligned to an organisation's existing password management policies. When the password has expired, the user will be presented with a Change Password window, whilst this is in place information in the Totalmobile app becomes inaccessible and unreadable. A notification of upcoming password change is also presented, ensuring that the user is made aware of the upcoming change requirement five days prior to the change being enforced.

Supplier and Third-Party Controls

Specific policy and process controls are in place to govern third-parties and suppliers, these include the establishment of contractual agreements with clauses around confidentiality and adherence to defined security controls as applicable.

Where a supplier or third-party are involved in the provision of services to a customer, for example hosting, then it is expected that they will hold the requisite certifications and comply to the same standards and apply the same security controls the customer requires of Totalmobile, with auditing of such certifications, compliance and security control application to be carried out where applicable.

HR and Personnel Security Controls

Information Security is instilled into our employees from the moment they commence their employment with Totalmobile. The induction process includes the signing of confidentiality agreements as part of their employment contract and the signing off of key policies such as Network Access and Acceptable Use and Clear Desk, Clear Screen Policies.

In conjunction with this, a dedicated information security training programme is in place that guides our staff through additional security policies and provides an overview of what information security means to Totalmobile, our partners and customers. These materials are centrally stored and are

accessible to all staff for reference. Assessments are in place on core training and awareness modules to ensure key requirements are understood by all employees.

User access management processes are also in place that govern access and privilege rights based on role and responsibility. This is applied in terms of granting, amending and revoking access permissions. This is managed via dedicated New Start and Leaver processes. Closely aligned with this is the assignment and reclaiming of equipment.

A background check and vetting is carried out prior to a new employee commencing work with Totalmobile and is also applied to tenured staff. Background checks typically include employment history, references, confirmation of academic or other qualifications required for a role, criminal and financial checks depending on the requirements of the role to be fulfilled and level of information and data that the member of staff will require or potentially have access to.

All security policies refer to the fact that non-adherence to the requirements of a policy or security control may result in disciplinary action, which could potentially result in dismissal. The Disciplinary Process specifically references information security considerations in the application of potential outcomes for disciplinary action.

Monitoring

The application and adherence to security controls are subject to both Internal and External auditing. External auditing is specifically carried out against our compliance to the ISO27001:2013 Standard and to the requirements of the NHS Digital Information Governance framework.

Internal audits are carried out on a departmental/functional basis considering specific controls dictated by applicable standards, contractual, legislative and regulatory requirements. Such internal audits are conducted by a dedicated, certified external Auditing Team. Outputs from internal and external audits are documented and used to leverage improvement initiatives within the ISMS and are also be used to identify and rectify potential issues in compliance or adherence to security requirements.