Flip Connect
GDPR Information Pack
Version 1.5 - January 2018

Flip Solutions Ltd t/a Flip Connect
The Maltings, Bridge Street,
Hitchin, Hertfordshire,
SG5 2DE

☎ 01462 417 100
0870 421 5411
hello@flipconnect.co.uk
www.flipconnect.co.uk

FLIPCONNECT™
Better . Connected

Contents

This page has intentionally been left Blank.

Introduction

In May 2018, the General Data Protection Regulation (EU) 2016/679 (GDPR) will come into force across the UK. GDPR in effect supersedes the Data Protection Act (DPA) 1998. GDPR moves away from the best practice approach of DPA towards enforceable regulations. As an example, Article 81 of GDPR states that the penalty for breaching the rules of the regulations can be up to 4% of turnover or €20 Million, depending on which is greater.

By superseding the DPA, GDPR introduces new conventions on Data Protection that both better protect individuals (known as natural persons) and organisations, as well as bestowing more rights to individuals, such as the right to be forgotten and the right for free movement of personal data.

According to the General Data Protection Regulation Article 1, the objectives of GDPR are as follows:

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

Flip Connect's clients (Controllers) are ultimately responsible for the implementation of GDPR within their own organisations and by extension have a legislative responsibility to ensure that third parties who process data on their behalf (Processors) are also compliant with the regulations as per GDPR Article 28 Paragraph 1

> *Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.*

Processing covers a wide variety of actions performed on personal data including, amongst others, the collection, storage and deletion of said data. According to GDPR Article 4, the definition of processing is as follows:

> *'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.*

These operations need to be protected by a robust set of technical and administrative measures, including the security of processing. Article 25 Paragraph 2 of GDPR defines the responsibilities of the Controller in ensuring that Data is protected by design and by default.

> *'The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons'.*

Flip Connect as a Processor ensures compliance with GDPR in respect to the protection of data through both appropriate technical and organisational measures. As such, Flip Connect is committed to protecting the rights and privacy of natural persons in accordance with GDPR with regard to the processing of personal data and on the free movement of such data.

In preparation for you undergoing a review of all your processors, Flip Connect intends to show its compliance by the publication of this information pack which consists of the following:

a. Name and Details of Organisation
b. Purposes of Processing
c. Personal Data Breaches
d. Policy Overview Diagram
e. Description of Policies and Procedures
f. In depth list of Information and Security controls (based upon ISO 27001 2013)
g. Retention of Data (extract from the Flip Connect Retention Policy)

Flip Connect will be fully compliant with all Policies and Procedures in accordance with the stipulated May 25th 2018 GDPR implementation timeline.

Please take the time to review the information pack and share with any focus groups within your organisation. We would appreciate your feedback, for which we will compile subsequent requests and will review and tailor a response accordingly.

Also, if you would like information on ways Flip Connect can assist you in producing outputs relating to the 'Right of Access' and the 'Right to restrict Data' or if you require any additional information please e-mail ben.smith@flipconnect.co.uk

Name and details of our organisation

Company Name:	Flip Solutions Ltd T/A Flip Connect
Company Registration Number:	4388417
Address:	The Maltings, Bridge Street, Hitchin, SG5 2DE
Telephone Number:	01462417100
Website:	www.flipconnect.co.uk
Email:	hello@flipconnect.co.uk

Purposes of Processing

In order for Flip Connect Ltd. to ensure that its contractual and legal obligations are adhered to, the 'processing' of client data is an essential requirement which falls within the stipulations of '*Article 6 Lawfulness of Processing*'.

This requirement can be broken down into four specific areas:

1. Problem Resolution and Prevention

2. Billing

3. Customisations

4. Projects

1. Problem Resolution

All customers with a current Service Agreement have access to the Flip Connect Helpdesk. The Helpdesk Service exists to ensure that all of our customers gain uninterrupted operational use of the services provided and make the best use of its various applications.

When a problem is reported, our helpdesk staff are trained to find out the circumstances that caused the issue to occur, on how the system was being used at the time, and which options and settings were selected and whether any changes had recently been made. If a solution cannot be provided immediately, the necessary testing and simulation work will be carried out to replicate the problem, for which access to the live system may be required, including the current database which contains personal data.

2. Billing

Services provided by Flip Connect will be subject to bill creation on a monthly and ad hoc basis. In order to provide detailed and accurate customer bills it is necessary for Flip Connect to store and access customers personal data.

3. Customisations

Customisations are work carried out specifically for an individual client and may include, for example, reports or Client specific enhancements. Customisations will generally require access to the customers live system, including the current database containing personal data.

4. Projects

By definition projects are items of work that fall within a longer duration than customisations, and to some degree require an aspect of project management. A project can range from a new feature, to the full-blown implementation of a new system. Projects will generally require a backup of a live system, including the current database containing personal data.

Access and storage of Personal Data

Achieving a successful outcome for the four areas identified above requires some or all of the underlying components:

Communication
Communication is a key element to the successful delivery of the four areas identified above. It can take the form of either verbal or electronic interaction (emails).

Recording of Information
All communication that requires an element of work to be done for Problem Resolution, Enhancement Requests or Customisations is stored in the Flip Connect ticket system. Within the ticket system the customer contact information, relevant attachments, and internal and external ticket information is recorded.

Customer specific folders are maintained within the Flip Connect IT network and may contain client information in relation to a specific issue or job.

Emails are accessed through Microsoft Outlook and are stored within the Microsoft office 365 servers.

Storage of Data
Flip Connect store customer data on various cloud servers and in some instances within a customer premise. Client data is securely transferred between servers for the purposes or processing when required. Hosted servers are all within the EU region.

Remote Access
Due to the client-server, web-enabled nature of Flip Connect, our Helpdesk operators can log in remotely to our client's systems over the Internet, to diagnose and investigate reported problems on your system from a PC in our own office. This makes it even easier for Flip Connect to provide a prompt response. It may be necessary at certain times to access the software using a third party remote access depending on the restrictions placed upon Flip Connect by our Client's IT Policies.

Software confidentiality and security will be adhered to at all times based on the Flip Connect Encryption Policy.

Personal Data Breaches

Introduction
To ensure Flip Connect Ltd. can efficiently conduct its business and meet its obligations under the Data Protection Act 1998 and the General Data Protection Regulation 2018, the effective and secure management of information is crucial.

All users of Flip Connect Ltd. information have a responsibility to:

- Minimise the risk of information being lost or disclosed to unauthorised individuals;
- Protect the security and integrity of IT systems or devices on which Flip Connect Ltd. information is held or processed;
- Ensure that physical security measures for protecting personal and sensitive information are adequate;
- Report actual or suspected information security incidents promptly so that appropriate action can be taken to mitigate risks and minimise potential harm to individuals and Flip Connect Ltd.

Purpose
The 'Flip Connect Staff Handbook explains the actions required in the event of an Information Security Incident, and sets out the responsibilities of all users of Flip Connect Ltd. data in respect of reporting and managing incidents.

Extracts from the policy follow:

In the event of an actual (or suspected) information security incident or breach, it is essential that Flip Connect Ltd. takes prompt action to mitigate the risks of potential harm to individuals, damage to operational business, and financial, legal and reputational costs. Where information security incidents are not reported, or where reports are delayed, the consequences can be severe and include:

- Damage or disruption to corporate systems;
- Damage and distress to individuals;
- Monetary penalties from regulators (including very significant fines for breaches of data protection);
- Harm to Flip Connect Ltd.'s reputation and subsequent erosion of trust;
- Loss of business assets;
- Increased risk of fraud or identity theft.

Scope and Definitions

The 'Flip Connect Staff Handbook forms part of Flip Connect Ltd.'s Information Security Framework. Overall responsibility for the policy lies with the Board of Directors.

This policy applies to:

- All information created or received by Flip Connect Ltd. in any format, whether held at the Hitchin Office or remotely, stored on desktop or static devices, or portable devices and media, whether transported from the workplace physically and electronically, or accessed remotely;
- Any incident that could have a detrimental effect on any Flip Connect Ltd. information assets or system;
- All users of Flip Connect Ltd.'s information and systems, including staff, visitors and contractors working on behalf of Flip Connect Ltd.;
- All Flip Connect Ltd. owned and managed IT systems;
- Any IT systems on which Flip Connect Ltd. information is held or processed, including personally owned devices;

An Information Security Incident can be defined as any event that poses a potential, suspected or actual threat to the security, confidentiality, integrity, or availability of Flip Connect Ltd. Information. Information Security Incidents can include:

- Intentional or accidental disclosure of any Flip Connect Ltd. data, in particular data of a confidential, high risk or sensitive nature of the type set out in the encryption policy, to anyone not authorised to view it;
- Loss or theft of paper records, data or equipment such as files, tablets, laptops, or smartphones on which data is stored;
- The execution of a malicious program designed to infiltrate and damage computers without the user's consent (e.g. malware or viruses from clicking on links or attachments in e-mails or from visiting compromised websites);
- Denial of service attacks (e.g. deliberate attempts to interrupt or suspend services of a host connected to the Internet);
- Security attacks on IT equipment systems or networks (e.g. hacking, malware and ransomware);
- Breaches of physical security that pose the threat of unauthorised access to sensitive Flip Connect Ltd. Information.

Incidents involving the receipt of spam or 'phishing' emails are also recognised as posing a threat to information security and these should be reported to IT.

Roles and Responsibilities

All users of Flip Connect Ltd.'s Information are responsible for reporting information security incidents. This includes actual, potential, and suspected incidents.

The Operations Director is responsible for ensuring all users of Flip Connect Ltd.'s Information are made aware of this policy, and for assisting with any investigations or incident management response as required.

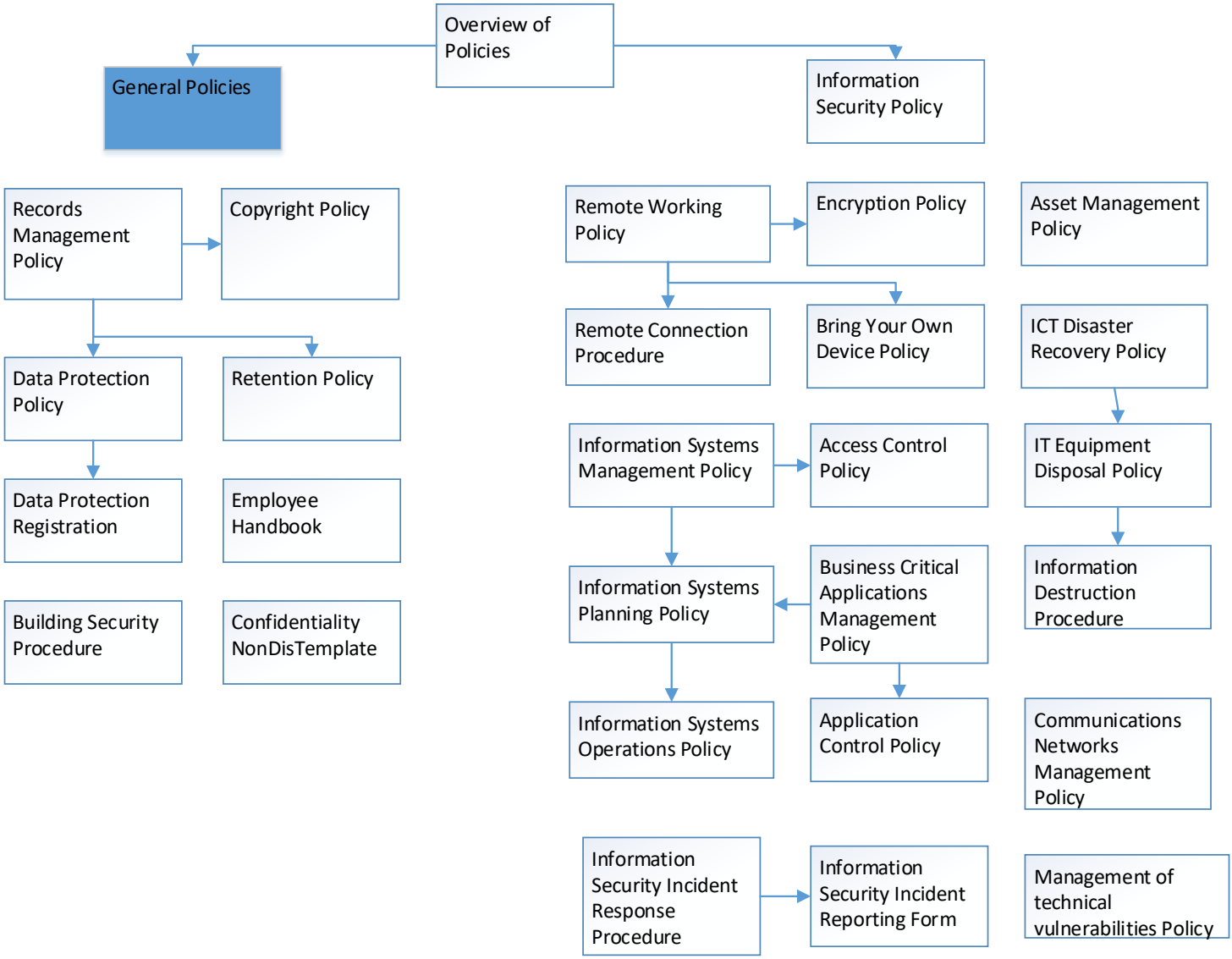
The Operations Director has overall responsibility for Information Management and ensuring effective governance of Information Management policies, procedures and training.

The Operations Director is responsible for: the communication and management of Information Security Incident reports; maintaining a central record of incidents reported and actions taken; advising on mitigations, changes to current practices and making best practice recommendations; co-ordination of incidents and advising on and completing notifications to the Information Commissioners Office (ICO).

Policy Procedures

The 'Flip Connect Staff Handbook' is to be used in conjunction with the 'Flip Connect Information Security Incident Response Procedure' and the 'Information_Security_Incident_Reporting_Form'.

Policy Overview Diagram



Description of Policies and Procedures

Purpose

This document aims to provide a quick overview of each policy relating to Information and Communication Management Systems, in particular those that are related to GDPR.

Policies

Flip Connect Retention Policy
For all staff and others who may process personal data on behalf of Flip Connect Ltd. to ensure that records (including documents and data) are retained in accordance with the Data Protection Act 1998 and GDPR 2018

Flip Connect Confidentiality Non-Disclosure Template
For all others excluding staff who may process or view personal data on behalf of Flip Connect Ltd. to ensure that they are compliant to and in accordance with the Data Protection Act 1998 and GDPR 2018

Flip Connect Asset Management Policy
This policy sets out the detailed procedures for the purchase, recording, transfer safeguarding and disposal of assets in Flip Connect Ltd.

Flip Connect Building Security Procedure
For all staff who have passed their probation period. This policy defines all aspects of building security including the management of keys, alarms and opening closing the office.

Flip Connect Data Protection Registration
For all staff and others who require details on Flip Connect Ltd.'s Data Protection registration.

Flip Connect Staff Handbook
For all staff to ensure their understanding of the company ethos and the breakdown of responsibilities between Flip Connect Ltd. and its employees.

Flip Connect Records Management Policy
For all staff, including any third parties conducting business on behalf of Flip Connect Ltd., to observe when managing Flip Connect Ltd. records. This policy provides the broad principles and guidelines to be applied to the management of records in Flip Connect Ltd. throughout their life cycle.

Flip Connect Data Protection Policy
For all staff and others who may process personal data on behalf of Flip Connect Ltd. to ensure that they are in accordance with the Data Protection Act 1998 and GDPR 2018. This policy ensures that all staff and others who process personal data on behalf of Flip Connect Ltd. are doing so in accordance with these principles at all times.

Flip Connect Copyright Policy
For members of staff and others who are working for, or on behalf of Flip Connect Ltd. to give guidance on the lawful use or copying of third party materials.

Flip Connect Information Security Policy
For all staff and others who process information, particularly sensitive information, on behalf of Flip Connect Ltd. to observe in order that all information they use is handled appropriately. This Policy forms part of Flip Connect Ltd.'s Information Framework. It also underpins other Flip Connect Ltd. policies, such as the Data Protection Policy which seeks to assure their compliance with relevant legislation.
It has a number of sub-policies which include:

> Flip Connect Access Control Policy
> For all staff who uses or accesses Flip Connect Ltd. systems or information. This policy establishes specific requirements for protecting information and information systems against unauthorised access.

Flip Connect Remote Working Policy
For anyone who use or access Flip Connect Ltd. systems or information remotely to ensure that they work in accordance with Flip Connect Ltd.'s information compliance policies. This policy provides guidance for staff on secure remote working and so minimises the risk of unauthorised access to, and loss of, data.

Flip Connect Encryption Policy
For anyone who processes sensitive information on external networks on behalf of the Flip Connect Ltd. This Policy sets out Flip Connect's policy on processing personal data and sensitive information, including the use of portable and mobile equipment.

Flip Connect Bring Your Own Device Policy
This policy applies to all Flip Connect Ltd. staff that process Flip Connect Ltd. data on personally owned devices. It sets out Flip Connect Ltd.'s policy on the use of personally owned devices to process Flip Connect Ltd. data and forms part of Flip Connect Ltd.'s Information Security Policy.

Flip Connect Communications Networks Management Policy
This policy applies to Flip Connect Ltd. IT staff responsible for the Communications Networks under the control of Flip Connect Ltd.

Flip Connect Information Systems Operations Policy
This policy applies to Flip Connect Ltd. IT staff that are responsible for areas and offices where sensitive or critical information is processed.

Flip Connect Business Critical Applications Management Policy
This is for all staff involved in software management.

Flip Connect Information Systems Management Policy
This is for IT staff involved in systems management. This policy identifies the management criteria for business critical applications.

Flip Connect Information Systems Planning Policy
For all IT staff involved in systems planning. This policy identifies the criteria for planning new information systems, or enhancements to existing systems.

Flip Connect Information Security Incident Response Procedures
This policy applies to all Flip Connect Ltd. staff. The purpose of this Policy is to provide instruction and guidance on reporting and managing information security incidents. Information security incidents are defined as those involving actual or potential compromise or disclosure of, and/or unauthorised access to, Flip Connect Ltd.'s data

Flip Connect Information Security Incident Reporting Form
This form provides details on incidents and is to be used in conjunction with the 'Flip Connect Information Security Incident Response Procedure' and 'Flip Connect Staff Handbook'.

Flip Connect ICT Disaster Recovery Policy
This policy enables Flip Connect to deal effectively with an ICT system disaster, thus ensuring that the effect, both short and long-term, of such an incident is minimised. It also provides guidance for Business Continuity in the event of Disaster Recovery.

Flip Connect Application Control Policy
For all staff as well as anyone who uses IT equipment. The primary purpose of this policy is to control the use of a minority of applications within Flip Connect Ltd.

Flip Connect Remote Connection Procedure
For all staff, including any third parties conducting business on behalf of Flip Connect Ltd. in order to comply the Data Protection Act 1998 and GDPR 2018. This document provides instructions for remotely connecting to the office network whilst ensuring correct security.

Flip Connect IT Equipment Disposal Policy
For all staff as well as anyone who uses IT equipment. This Policy sets out Flip Connect Ltd.'s policy on the disposal of computer equipment and data storing devices.

Flip Connect Information Destruction Procedure
This procedure defines how information-bearing media (i.e. Paper and Hard Drives) must be destroyed prior to disposal.

Flip Connect Management of Technical Vulnerabilities Policy
This policy applies to Flip Connect Ltd's IT staff that are responsible for areas and offices where sensitive or critical information is processed. This Policy defines the minimum security controls for Information Technology systems in use at Flip Connect Ltd.

Information Security Controls

The following table is based upon ISO/IEC 27001 second edition 2013-10-01

Objective	Description	Notes
Management direction for information security	To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.	
Policies for information security	A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.	Flip Connect maintain a comprehensive set of Data Protection and Information Security policies which are summarised within this document.
Review of the policies for information Security	The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	Flip Connect maintain a comprehensive set of Data Protection and Information Security policies which are reviewed annually. All such policies and procedures are communicated to employees on a regular basis.
Internal organisation	Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organisation.	
Information security roles and responsibilities	All information security responsibilities shall be defined and allocated.	As defined by the Flip Connect Information Security Policy and the Staff Handbook.
Segregation of duties	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets.	Flip Connect Information Systems Operations Policy
Contact with authorities	Appropriate contacts with relevant authorities shall be maintained.	n/a
Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.	n/a
Information security in project management	Information security shall be addressed in project management, regardless of the type of the project.	Flip Connect Data Protection Policy states that Flip Connect Ltd. will process personal data and manage the free movement of such data in accordance with the Data Protection Principles that are set out in the GDPR. This covers all projects undertaken with our clients.
Mobile devices and teleworking (Homeworking)	To ensure the security of teleworking and use of mobile devices.	

Mobile device policy	A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.	Flip Connect Remote Working Policy
Human resource security	To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.	
Terms and conditions of employment	The contractual agreements with employees and contractors shall state their and the organisation's responsibilities for information security.	Included as part of the induction programme and enshrined within the Employees Handbook
During employment	To ensure that employees and contractors are aware of and fulfil their information security responsibilities.	Flip Connect maintain a comprehensive set of Data Protection and Information Security policies which are reviewed annually. All such policies and procedures are communicated to employees on a regular basis. In addition, Employee responsibilities are defined in the Staff Handbook.
Management responsibilities	Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organisation.	Flip Connect Management require that all employees and contractors adhere to all the established policies and procedures of the organisation.
Information security awareness, education and training	All employees of the organisation and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organisational policies and procedures, as relevant for their job function.	Flip Connect maintain a comprehensive set of Data Protection and Information Security policies which are reviewed annually. All such policies and procedures are communicated to employees on a regular basis. In addition, Employee responsibilities are defined in the Staff Handbook.
Disciplinary process	There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.	The disciplinary process is defined in the Staff Handbook. The Data Protection and Information Security policies define in further detail the risks associated with information security breaches and state that disciplinary proceeding can be taken against employees who are deemed to be in breach of these policies.
Termination and change of employment	To protect the organisation's interests as part of the process of changing or terminating employment.	
Termination or change of employment responsibilities	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.	Specified in the Staff Handbook
Responsibility for assets	To identify organisational assets and define appropriate protection responsibilities.	

Inventory of assets	Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.	Fixed asset register as defined in the Flip Connect Asset Management Policy
Ownership of assets	Assets maintained in the inventory shall be owned.	As defined in the fixed asset register as part of the Flip Connect Asset Management Policy
Acceptable use of assets	Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.	The Flip Connect Staff Handbook ensures that Flip Connect Ltd.'s IT facilities are used safely, securely, lawfully and equitably.
Return of assets	All employees and external party users shall return all of the organisational assets in their possession upon termination of their employment, contract or agreement.	Specified in the Staff Handbook.
Audit of Information	Evaluation of who/what/why/when/where data comes from and have mechanism in place to retain/delete	As defined in Audit of information document.
Media handling	To prevent unauthorised disclosure, modification, removal or destruction of information stored on media.	
Management of removable media	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organisation.	The Flip Connect Staff Handbook ensures that Flip Connect Ltd.'s IT facilities are used safely, securely, lawfully and equitably.
Disposal of media	Media shall be disposed of securely when no longer required, using formal procedures.	Flip Connect IT Equipment Disposal Policy which sets out Flip Connect Ltd.'s policy on the disposal of computer equipment and data storing devices.
Physical media transfer	Media containing information shall be protected against unauthorised access, misuse or corruption during transportation.	Flip Connect Encryption Policy sets out Flip Connect's policy on processing personal data and sensitive information, including the use of portable and mobile equipment.
Business requirements of access control	To limit access to information and information processing facilities.	
Access control policy	An access control policy shall be established, documented and reviewed based on business and information security requirements.	Flip Connect Access Control Policy establishes specific requirements for protecting information and information systems against unauthorised access.
Access to networks and network services	Users shall only be provided with access to the network and network services that they have been specifically authorized to use.	Flip Connect Access Control Policy establishes specific requirements for protecting information and information systems against unauthorised access including networks and network services.
User access management	To ensure authorized user access and to prevent unauthorised access to systems and services.	

User registration and de-registration	A formal user registration and de-registration process shall be implemented to enable assignment of access rights.	Flip Connect Access Control Policy establishes specific requirements for protecting information and information systems against unauthorised access including user registration and de-registration
User access provisioning	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.	Flip Connect Access Control Policy establishes specific requirements for protecting information and information systems against unauthorised access.
Management of privileged access rights	The allocation and use of privileged access rights shall be restricted and controlled.	Flip Connect Access Control Policy establishes specific requirements for protecting information and information systems against unauthorised access including management of privileged access rights.
Review of user access rights	Asset owners shall review users' access rights at regular intervals.	Flip Connect Access Control Policy establishes specific requirements for protecting information and information systems against unauthorised access including the review by business owners on user access rights.
Removal or adjustment of access rights	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	Flip Connect Access Control Policy establishes specific requirements for protecting information and information systems against unauthorised access including the removal of access rights where deemed necessary.
User responsibilities	To make users accountable for safeguarding their authentication information.	
Use of secret authentication information	Users shall be required to follow the organisation's practices in the use of secret authentication information.	The Flip Connect Staff Handbook ensures that Flip Connect Ltd.'s IT facilities are used safely, securely, lawfully and equitably.
System and application access control	To prevent unauthorised access to systems and applications.	
Information access restriction	Access to information and application system functions shall be restricted in accordance with the access control policy.	Flip Connect Access Control Policy establishes specific requirements for protecting information and information systems against unauthorised access including the review by business owners on user access rights.
Secure log-on procedures	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.	As defined in the Flip Connect Access Control Policy and the Administering User Accounts Procedure.
Cryptographic controls	To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.	

Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	The Flip Connect Encryption Policy sets out Flip Connect's policy on processing personal data and sensitive information, including the use of portable and mobile equipment along with required encryption standards.
Key management	A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.	Key Management is defined in the Flip Connect Building Security Procedure.
Physical and environmental security	To prevent unauthorised physical access, damage and interference to the organisation's information and information processing facilities.	Physical and environmental security is defined in the Flip Connect Building Security Procedure.
Working in secure areas	Procedures for working in secure areas shall be designed and applied.	Physical and environmental security is defined in the Flip Connect Building Security Procedure.
Protecting against external and environmental threats	Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.	The Flip Connect Information Security Response Policy explains the actions required in the event of an Information Security Incident, and sets out the responsibilities of all users of Flip Connect Ltd. data in respect of reporting and managing incidents in conjunction with the relevant document Flip Connect Information Security Incident Response Procedure. The Flip Connect ICT Disaster Recovery policy enables Flip Connect to deal effectively with an ICT system disaster.
Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and applied.	Physical and environmental security is defined in the Flip Connect Building Security Procedure
Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	Physical and environmental security is defined in the Flip Connect Building Security Procedure
Equipment	To prevent loss, damage, theft or compromise of assets and interruption to the organisation's operations.	
Equipment maintenance	Equipment shall be correctly maintained to ensure its continued availability and integrity.	As defined in the Information Systems Management Policy with a detailed description of tasks in the IT Tasks log file.
Removal of assets	Equipment, information or software shall not be taken off-site without prior authorization.	The Flip Connect Remote Working Policy ensures that staff are aware of their individual responsibilities around information security when working remotely.
Security of equipment and assets off-premises	Security shall be applied to off-site assets taking into account the different risks of working outside the organisation's premises.	The Flip Connect Remote Working Policy ensures that staff are aware of their individual responsibilities around information security when

		working remotely including security of their equipment.
Secure disposal or reuse of equipment	All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	The Flip Connect IT Equipment Disposal Policy sets out Flip Connect Ltd.'s policy on the disposal of computer equipment and data storing devices.
Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection.	The Flip Connect Staff Handbook ensures that Users are responsible for unattended computer security.
Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.	The Flip Connect Staff Handbook states that Flip Connect Ltd. employs a clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities.
Operational procedures and responsibilities	To ensure correct and secure operations of information processing facilities.	
Documented operating procedures	Operating procedures shall be documented and made available to all users who need them.	Specified in the GDPR Operating Procedures.doc
Capacity management	The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	As defined in the Flip Connect Information Systems Management Policy which states that capacity demands of systems supporting business processes shall be monitored and projections of future capacity requirements made to enable adequate processing power, storage and network capacity to be made available.
Protection from malware	To ensure that information and information processing facilities are protected against malware.	
Controls against malware	Detection, prevention and recovery controls to protect against malware shall be implemented and combined with appropriate user awareness.	The Flip Connect Staff Handbook ensures that Users must take all reasonable steps to avoid introducing malware to the infrastructure. The Flip Connect Information Systems Management Policy identifies that all Flip Connect Ltd.'s systems shall be protected from virus and other malicious software infection using software and hardware products procured by Flip Connect Ltd. for this purpose.
Backup	To protect against loss of data.	

Information backup	Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.	The Flip Connect Information Systems Management Policy identifies the need that data and software can be recovered following a media failure or computer disaster, backup copies of all essential data and software must be regularly taken.
Logging and monitoring	To record events and generate evidence.	
Event logging	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	The Flip Connect Information Systems Management Policy identifies that Security event logs, operational audit logs and error logs must be properly and periodically reviewed.
Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorised access.	The Flip Connect information Systems Management Policy states that security event logs, operational audit logs and error logs must be properly and periodically reviewed and access restricted to those persons who are authorised to perform systems administration or management functions.
Administrator and operator logs	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	The Flip Connect information Systems Management Policy states that security event logs, operational audit logs and error logs must be properly and periodically reviewed.
Clock synchronisation	The clocks of all relevant information processing systems within an organisation or security domain shall be synchronised to a single reference time source.	The Flip Connect information Systems Management Policy states that system clocks must be regularly synchronised between Flip Connect Ltd.'s various processing platforms.
Control of operational software	To ensure the integrity of operational systems.	
Installation of software on operational systems	Procedures shall be implemented to control the installation of software on operational systems.	Defined in the Flip Connect Information Systems Management Policy which states that the implementation of new or upgraded software must be carefully planned and managed.
Technical vulnerability management	To prevent exploitation of technical vulnerabilities.	
Management of technical vulnerabilities	Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organisation's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	Defined in the Flip Connect Management of Technical Vulnerabilities Policy

Restrictions on software installation	Rules governing the installation of software by users shall be established and implemented.	Within the Staff Handbook it states that only software packages properly authorised and installed by the Company may be used on Company equipment, you must therefore not load any unauthorised software onto Company computers'.
Network security management	To ensure the protection of information in networks and its supporting information processing facilities.	
Network controls	Networks shall be managed and controlled to protect information in systems and applications.	Flip Connect Access Control Policy Flip Connect Application Control Policy
Segregation in networks	Groups of information services, users and information systems shall be segregated on networks.	There is no segregation of networks - Flip Connect financial data is separated on an isolated server.
Information transfer	To maintain the security of information transferred within an organisation and with any external entity.	
Information transfer policies and procedures	Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.	The Flip Connect Encryption Policy sets out Flip Connect's policy on processing personal data and sensitive information, including the use of portable and mobile equipment along with required encryption standards.
Agreements on information transfer	Agreements shall address the secure transfer of business information between the organisation and external parties.	On a per client basis.
Electronic messaging	Information involved in electronic messaging shall be appropriately protected.	Flip Connect Encryption Policy states that high risk personal data or sensitive information should be sent using the FTPS or SFTP as defined in the 'Guide to the new file transfer platform, within this guide it states that all confidential data should be encrypted and password protected. The Flip Connect Encryption Policy also states that if you must use email to send this sort of information, encrypt it and password protect it.
Confidentiality or nondisclosure agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information shall be identified, regularly reviewed and documented.	Flip Connect maintains the non-disclosure agreement template Flip Connect Confidentiality Non-Disclosure Template.
Security requirements of information systems	To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.	

Information security requirements analysis and specification	The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.	Requirements are defined in the Information Systems Planning Policy.
Securing application services on public networks	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorised disclosure and modification.	The security mechanisms of Flip Connect World Service are defined in 'Flip Connect World Service Security.docx'. Within the Flip Connect Encryption policy it is stated that remote sessions should only be established using approved applications such as RDP and LogMeIn. These sessions should be established over TLS 1.1 or greater. SFTP runs over SSH in the standard SSH port while FTPS utilises TLS 1.1 or greater.
Protecting application services transactions	Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay.	The security mechanisms of Flip Connect World Service are defined in 'Flip Connect World Service Security.docx'. Within the Flip Connect Encryption policy it is stated that remote sessions should only be established using approved applications such as RDP and LogMeIn. These sessions should be established over TLS 1.1 or greater. SFTP runs over SSH in the standard SSH port while FTPS utilises TLS 1.1 or greater.
Management of information security incidents and improvements	To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.	
Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.	Management responsibility is defined in the Flip Connect Staff Handbook.
Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.	As defined in the Flip Connect Information Security Incident Response Procedure which provides instruction and guidance on reporting and managing information security incidents.
Reporting information security weaknesses	Employees and contractors using the organisation's information systems and services shall be required to note and report any	The Flip Connect Staff Handbook states that all users of Flip Connect Ltd.'s Information are responsible for reporting information security

	observed or suspected information security weaknesses in systems or services.	incidents. This includes actual, potential, and suspected incidents.
Assessment of and decision on information security events	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.	The Flip Connect Staff Handbook states that on notification of a Security Incident the Operations Director will make initial assessments, take any immediate remedial actions necessary to contain and recover as necessary.
Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	The Flip Connect Information Security Incident Response Procedure provides instruction and guidance on reporting and managing information security incidents.
Learning from information security incidents	Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.	The Flip Connect Staff Handbook stipulates that all reasonable endeavours shall be made to ensure that appropriate technical and organisational measures are taken to ensure the security and integrity of Flip Connect Ltd.'s data, which includes the learning from information security incidents.
Collection of evidence	The organisation shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	The Flip Connect Staff Handbook stipulates that all incidents reported will be recorded centrally and maintained by the Operations Director.
Information security continuity	Information security continuity shall be embedded in the organisation's business continuity management systems.	
Planning information security continuity	The organisation shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.	The Flip Connect Staff Handbook identifies the need that data and software can be recovered following a media failure or computer disaster, backup copies of all essential data and software must be regularly taken. The Flip Connect ICT Disaster Recovery Policy enables Flip Connect to deal effectively with an ICT system disaster.
Implementing information security continuity	The organisation shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	The Flip Connect ICT Disaster Recovery Policy enables Flip Connect to deal effectively with an ICT system disaster.
Verify, review and evaluate information security continuity	The organisation shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.	The Flip Connect ICT Disaster Recovery Policy enables Flip Connect to deal effectively with an ICT system disaster. The Flip Connect Staff Handbook and the Flip Connect Information Security Incident Response Procedure sets out the responsibilities of all users of Flip Connect Ltd. data in respect

		of reporting and managing information related incidents.
Redundancy	To ensure availability of information processing facilities.	
Availability of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	The Flip Connect Information Systems Management Policy states that information processing facilities shall be implemented with redundancy sufficient to meet availability requirements, either through redundancy of functions or load sharing across different hardware.
Compliance with legal and contractual requirements		Flip Connect Ltd. is committed to protecting the rights and privacy of individuals in accordance with Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) which is also known as GDPR.
Identification of applicable legislation and contractual requirements	All relevant legislative statutory, regulatory, contractual requirements and the organisation's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organisation.	Achieved through a set of comprehensive Data Protection and Information Security policies in line with The Data Protection Act and GDPR.
Intellectual property rights	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.	As defined in the Flip Connect Copyright Policy.
Protection of records	Records shall be protected from loss, destruction, falsification, unauthorised access and unauthorised release, in accordance with legislatory, regulatory, contractual and business requirements.	The Flip Connect Records Management Policy provides the broad principles and guidelines to be applied to the management of records in Flip Connect Ltd. throughout their life cycle.
Privacy and protection of personally identifiable information	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.	Flip Connect Ltd. is committed to protecting the rights and privacy of individuals in accordance with Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) which is also known as GDPR.

Regulation of cryptographic controls	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.	The Flip Connect Encryption Policy ensures that if high risk personal data or sensitive information is to be processed then it must be stored and transmitted in an encrypted form of the required standard.

Retention of Data

Record	Statutory Retention Period	Regulation	Recommended Retention Period	Remarks
Client Backups				
Support	N/A	N/A	12 Months	Backups older than 12 months automatically deleted using SharePoint workflows
Project	N/A	N/A	12 Months	Backups older than 12 months automatically deleted using SharePoint workflows
One off Commercial	N/A	N/A	12 Months	Backups older than 12 months automatically deleted using SharePoint workflows
Hosted Databases				
Service	N/A	N/A	Permanently	
CRM system				
Contact Info	N/A	N/A	Permanently	
Attachments	N/A	N/A	5 years	Attachments older than 5 years automatically deleted using CRM workflow
Ticket information	N/A	N/A	5 years	Attachments older than 5 years automatically deleted using CRM workflow
Commercial	N/A	N/A	Permanently	
Xero	N/A	N/A	Permanently	
E-mails				
Support	N/A	N/A	5 years	
Project	N/A	N/A	5 years	
Service	N/A	N/A	5 years	
Commercial	N/A	N/A	Permanently	
Folder Structure				
Support	N/A	N/A	5 years	
Project	N/A	N/A	5 years	
Service	N/A	N/A	5 years	
Commercial	N/A	N/A	Permanently	
Hard Copies				
Notepads	N/A	N/A	N/A	Clear Screen and Desk Policy
Prints	N/A	N/A	N/A	Clear Screen and Desk Policy
Whiteboards	N/A	N/A	N/A	Clear Screen and Desk Policy