Statement of Applicability

Clause	Control Objective / Control	Sec / Clause	Control in place	Justification / Remarks
1. Information security Policies	**Management direction for information security**	**1.1**	**Objective:**	**To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.**
	Policies for Information Security	1.1.1	Yes	We have a set of policies that are approved by Board that are referenced in this Statement of Applicability. We also have a high-level global framework and policy for Information Security to support our Quality Management and Cyber Security. This applies to all team members and contractors in the UK.
	Review of the policies for information security	1.1.2	Yes	All our policies follow a standard format which includes details of the policy owner(s) coordinator(s) & approver(s). All policies reviewed annually or sooner if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.
2. Organisation of information security	**Internal organisation**	**2.1**	**Objective:**	**To establish a management framework to initiate and control the implementation and operation of information security within the organization.**
	Information Security Roles and Responsibilities	2.1.1	Yes	Responsibility and accountability for the management of our system resides with our Managing Director. The Managing Director has overall responsibility with delegation to our Operational Team. Individual assets have owners designated in the asset register.
	Segregation of Duties	2.1.2	Yes	Our Access Control is to ensure that conflicting duties and areas of responsibility are segregated.
	Contact with Authorities	2.1.3	Yes	We maintain contact with relevant law enforcement and regulatory bodies both in the normal course of our business and in exceptional circumstance to report security incidents or to maintain continuity of our business.
	Contact with Special Interest Groups	2.1.4	Yes	We are members of various professional bodies and conform to a number of regulatory frameworks.
	Information Security with Project Management	2.1.5	Yes	We address information security in all projects, Information security implications are expected to be addressed and reviewed regularly in all projects.
	Mobile Devices and Teleworking	**2.2**	**Objective:**	**To ensure the security of teleworking and use of mobile devices.**
	Mobile Device Policy	2.2.1	Yes	Mobile devices (including Smart Phones and Tablets) are widely used in our organisation. The requirements for both

				company provided devices and employee owned devices are set out in our policies. Training is provided to reinforce understanding and compliance.
	Teleworking	2.2.2	Yes	Teleworking is common practice in our modern working environment. Our policies and training take into account the risks and associated controls required.
3. Human Resource Security	**Prior to Employment**	**3.1**	**Objective:**	**To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.**
	Screening	3.1.1	Yes	Background verification checks in line with our policy and procedure are carried out for all candidates for employment. The policy takes account of relevant laws and regulations; is proportional to the business requirements, the classification of the information to be accessed and the perceived risks to the business. We have contractual agreements with third party suppliers whose employees work at our premises are often referred to as contractors. Our supplier agreements with these third parties require their employees to comply with our Information Security policies and procedures.
	Terms & Conditions of Employment	3.1.2	Yes	The contractual obligations for employees and contractors engaged by In-Form Solutions are set out in the Terms & Conditions of Employment which all employees and directly employed contractors are required to sign before commencing employment. These terms and conditions also set out the continuing responsibilities for Information Security after employment ends. We have contractual agreements with third party suppliers whose employees work at In-Form Solutions premises are often referred to as contractors. Our supplier agreements with these third parties require their employees to comply with our Information Security policies and procedures.
	During Employment	**3.2**	**Objective:**	**To ensure that employees and contractors are aware of and fulfil their information security responsibilities.**
	Management Responsibility	3.2.1	Yes	Being 'Data Inspired' is one of In-Form Solutions' core values and the importance of data and information security is part of the culture of our

				business. All new employees are assessed against their terms & conditions of employment, their information security obligations and other criteria during their probationary period and throughout their employment. Management ensure that employees are trained in aspects of information security relevant to their role. We have a clear Whistleblowing Policy.
	Information Security Awareness, Education and Training	3.2.2	Yes	A program of general Information Security Awareness, Education & Training exists for all employees. Where there are role specific information security requirements, training needs are assessed and appropriate training arranged.
	Disciplinary process	3.2.3	Yes	We have a clear Disciplinary Policy and Procedure to handle circumstances where an employee who has committed an information security breach.
	Termination and Change of Employment	**3.3**	**Objective:**	**To protect the organization's interests as part of the process of changing or terminating employment.**
	Termination or Change of Employment Responsibilities	3.3.1	Yes	Processes exist to ensure employees are reminded of their obligations with regard to information security and the consequences of not meeting those obligations when they leave In-Form Solutions.
4. Asset Management	**Responsibility for Assets**	**4.1**	**Objective:**	**To identify organizational assets and define appropriate protection responsibilities.**
	Inventory of assets	4.1.1	Yes	We have an Inventory of information security related assets contained in our Asset Register.
	Ownership of Assets	4.1.2	Yes	All information security related assets (or groups of assets) have designated owners who are responsible for the asset throughout its lifecycle or owners for defined phases of the asset's lifecycle.
	Acceptable use of Assets	4.1.3	Yes	Acceptable use of Information Security related assets is defined in a number of our policies, including our Data Protection Policy, Data Retention Policy, Employees' Data Protection Policy and Privacy Policy and is reinforced through training and awareness courses.
	Return of Assets	4.1.4	Yes	Procedures are in place to ensure that Information Security related assets that are assigned to employees or contractors are returned when the contract with the employee or contractor ends.
	Media Handling	**4.2**	**Objective:**	**To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.**

	Management of Removable Media	4.2.1	Yes	The use, management and destruction of removable media is controlled by our Data Protection Policy.
	Disposal of Media	4.2.2	Yes	Disk drives for media storage is disposed of in accordance to our Data Retention Policy.
5. Access Control	**Business Requirements of Access Control**	**5.1**	**Objective:**	**To limit access to information and information processing facilities.**
	Access Control Policy	5.1.1	Yes	Access to the network and systems is authorised by the Board.
	Access to Networks and Network Services	5.1.2	Yes	Access to the network and systems is authorised by the Board.
	Business Requirements of Access Control	**5.2**	**Objective:**	**To ensure authorized user access and to prevent unauthorized access to systems and services.**
	User Registration and De-Registration	5.2.1	Yes	There are policies and standards in place, and a formal user registration and de-registration procedure for granting and revoking access to all information technology systems and services.
	User Access Provisioning	5.2.2	Yes	Formal user access provisioning process is implemented to assign access rights for all user types to all systems and services and is authorised by a Board member.
	Management of Privileged Access Rights	5.2.3	Yes	Allocation and use of privileges are restricted by authorisation of the Board.
	Management of Secret Authentication Information of Users	5.2.4	Yes	Allocation of passwords is controlled through a formal management process.
	User Responsibilities	**5.3**	**Objective:**	**To make users accountable for safeguarding their authentication information.**
	Use of Secret Authentication Information	5.3.1	Yes	A Confidentiality Agreement is included in employee's terms and conditions of employment.
	System and Application Access Control	**5.4**	**Objective:**	**To prevent unauthorized access to systems and applications.**
	Information Access Restriction	5.4.1	Yes	Access to information and application system functions by users and support personnel is restricted in accordance with our Privacy Policy.
	Secure Log-on Procedures	5.4.2	Yes	Access to operating systems is controlled by a secure log-on policy.
	Password Management System	5.4.3	Yes	Systems for managing password is interactive and ensure quality password.
	Access control to program Source Code	5.4.4	Yes	Access to program source code is restricted.
7. Physical and Environmental Security	**Secure Areas**	**6.1**	**Objective:**	**To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.**

	Physical Security Perimeter	6.1.1	Yes	In-From Solutions' offices are in a secure working environment with locks and effective backup solutions.
	Physical Entry Controls	6.1.2	Yes	All employees require a key-card and key-fob to access the premises.
	Securing Offices, Rooms and Facilities	6.1.3	Yes	Secured information processing faculties are identified and secured by access control systems.
	Protecting against External and Environmental Threats	6.1.4	Yes	Protection of our facilities, in line with health and safety legislation requirements, is in place. Additional fire, heat and flood protection is active in sensitive secure areas housing essential equipment. Additional security measures are also in place at all our sites to help prevent malicious access.
	Working in Secure Areas	6.1.5	Yes	We have policies and procedures to ensure that access to secure areas is restricted on a specific needs basis and that special working procedures are in place and rigorously enforced.
	Delivery and Loading Areas	6.1.6	Yes	All deliveries are made via dedicated reception teams.
	Equipment	**6.2**	**Objective:**	**To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.**
	Equipment Sighting and Protection	6.2.1	Yes	Equipment is sited or protected to reduce the risks from environmental threats and hazards and opportunities for unauthorised access.
	Supporting Utilities	6.2.2	Yes	Equipment is protected from power failures and other disruptions caused by failures in supporting utilities by ensuring suitable planning and architecture of infrastructure utilities.
	Cabling Security	6.2.3	Yes	Power and telecommunication cabling carrying data or supporting information services is protected from interruptions or damaged.
	Equipment Maintenance	6.2.4	Yes	Equipment is correctly maintained to ensure its continued availability and integrity.
	Removal of Assets	6.2.5	Yes	Equipment, information and software is not be taken off-site without prior authorisation of their manager unless set out in policy.
	Security of Equipment and Assets Off-Premises	6.2.6	Yes	Security is applied to assets and equipment off-site, considering the different risks that arise outside the premises.
	Secure Disposal or Re Use of Equipment	6.2.7	Yes	Policy, process and procedures exist that ensure that all equipment reuse is managed and is disposed of securely.
	Unattended User Equipment	6.2.8	Yes	Policy, standards and training are in place to ensure that users log off or lock devices whenever equipment is left unattended so that passwords or PINs are required to reactivate sessions and that sessions should be terminated when no longer in use.

	Clear Desk and Screen Policy	6.2.9	Yes	Policy, standards and training are in place to ensure that users clear their desk of restricted information when unattended and log off or lock devices whenever equipment is left unattended so that passwords or PINs are required to reactivate sessions.
8. Operations Security	**Operational Procedures and responsibilities**	**7.1**	**Objective:**	**To ensure correct and secure operations of information processing facilities.**
	Documented Operating Procedures	7.1.1	Yes	Procedures, policies (containing procedures), training materials and other instructions / information is provided to those that need them to effectively fulfil the information security aspects of their roles.
	Change Management	7.1.2	Yes	Policies and processes are documented to ensure that changes likely to impact information security are controlled.
	Capacity Management	7.1.3	Yes	Use of resources is monitored, tuned and projections made of future capacity requirements to ensure the required system performance.
	Protection from Malware	**7.2**	**Objective:**	**To ensure that information and information processing facilities are protected against malware.**
	Controls against Malware	7.2.1	Yes	Where technically feasible, all servers and workstations are required to have active anti-malware software that is configured in compliance with our standards. Any server or workstation without active malware configured any-malware software may be blocked from network services until brought into compliance.
	Back-Up	**7.3**	**Objective:**	**To protect against loss of data.**
	Information Backup	7.3.1	Yes	Back-up copies of information and software are taken and tested regularly in accordance with the agreed back-up routine. There are four separate daily back-ups.
	Logging and Monitoring	**7.4**	**Objective:**	**To record events and generate evidence.**
	Event Logging	7.4.1	Yes	Audit logs recording user activities, exceptions and information security incidents is produced and kept for an agreed time period to assist future investigations and access control monitoring.
	Protection of Log Information	7.4.2	Yes	Logging facilities and log information is protected against tampering, unauthorised access and destruction.
	Administrator and Operator Logs	7.4.3	Yes	System Administrator/Operator activities is logged, protected from amendment by the same System/Operator Administrator and regularly reviewed.
	Control of Operational Software	**7.5**	**Objective:**	**To ensure the integrity of operational systems.**
	Installation of software	7.5.1	Yes	We have policies and procedures in place to ensure the installation of

	on Operational Systems			software on production systems is appropriately controlled.
	Technical Vulnerability Management	**7.6**	**Objective:**	**To prevent exploitation of technical vulnerabilities.**
	Management of Technical Vulnerabilities	7.6.1	Yes	Technical vulnerabilities are identified and managed in line with our policies and processes.
	Restrictions on Software Installations	7.6.2	Yes	Only approved, licensed and functionally required software is installed on end user devices.
	Information Systems Audit Considerations	**7.7**	**Objective:**	**To minimise the impact of audit activities on operational systems.**
	Information System Audit Controls	7.7.1	Yes	Security documents set out compliance requirements in all policies, standards, procedures, etc., so that implementers & management know what they will be measured against. Technical tests are included in the compliance section as well.
9. Communications Security	**Network Security Management**	**8.1**	**Objective:**	**To ensure the protection of information in networks and its supporting information processing facilities.**
	Network Controls	8.1.1	Yes	In-Form Solutions maintain appropriate controls and procedures to ensure the consistent and secure operations of the network and related components.
	Security of Network Services	8.1.2	Yes	In-Form Solutions ensure security is considered and addressed in all network service agreements.
	Segregation in Networks	8.1.3	Yes	Networks are segregated as much as practical to prevent access overlap and to minimise impact of any incident to a network.
	Information Transfer	**8.2**	**Objective:**	**To maintain the security of information transferred within an organisation and with any external entity.**
	Information Transfer Policies and Procedures	8.2.1	Yes	Formal transfer policies, procedures and controls are in place to protect the transfer of information using all types of communication facilities.
	Agreements on Information Transfer	8.2.2	Yes	Agreements are in place between In-Form Solutions and third-party vendors and business partners.
	Electronic Messaging	8.2.3	Yes	Information involved in electronic messaging is appropriately protected.
	Confidentiality or Non-Disclosure Agreements	8.2.4	Yes	Confidentiality and non-disclosure agreements are established and used where appropriate to protect information.
10. System Acquisition, Development and Maintenance	**System Requirements of Information Systems**	**9.1**	**Objective:**	**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	9.1.1	Yes	Statements of business requirements for new and information technology systems, or enhancements to existing

	Requirements Analysis and Specifications			information technology systems specify the requirements for security controls.
	Securing Application Services on Public Networks	9.1.2	Yes	All systems and supporting infrastructure that engage in e-commerce is designed, developed and operated in a manner that appropriately protects the interests of In-Form Solutions and its customers.
	Protection Application Services Transactions	9.1.3	Yes	Information involved in application service interactions is protected to ensure that its confidentiality, availability and integrity is, by design and overall architecture, protected.
	Security in Development and Support	**9.2**	**Objective:**	**To ensure that information security is designed and implemented within the development lifecycle of information systems.**
	Secure Development Policy	9.2.1	Yes	Development of software within the organisation is set out in our policy for secure application development. We have Support Service Agreements with specialist contractors. Third Parties are required to meet our standards as set out in our Third-Party Management Policy.
	System Change Controls Procedures	9.2.2	Yes	System changes are controlled by policies and implemented following process and procedure.
	Technical Review of Applications after Operating Platform Changes	9.2.3	Yes	When operating platforms are changed, business critical applications are reviewed and tested to ensure no adverse reactions to operations or security.
	Restrictions on changes to Software Packages	9.2.4	Yes	Changes to software packages are discouraged, limited to necessary changes and effective software change control.
	System Security Testing	9.2.5	Yes	Systems security requirements and functionality are integrated into software test plans.
	System Acceptance Testing	9.2.6	Yes	Software change control, test procedures and system acceptance procedures are followed when new or amended hardware, software and relevant procedures are introduced to the production environment.
11. Supplier Relationships	**Information Security in Supplier Relationships**	**10.1**	**Objective:**	**To ensure protection of the organisation's assets that is accessible by suppliers.**
	Information Security Policy for Supplier Relationships	10.1.1	Yes	Through agreements and contracts we require our vendors to meet Information Security requirements as set out in relevant policies.
	Addressing Security with Supplier Agreements	10.1.2	Yes	Appropriate arrangements are in place in relation to information security agreements with third-party vendors and Business Partners.
	Information and Communication Technology Supply	10.1.3	Yes	Agreements with vendors include requirements that address the

	Chain			information security risks associated with information and communication technology services and product supply chain.
	Supplier Service Delivery Management	**10.2**	**Objective:**	**To maintain an agreed level of information security and service delivery in line with supplier agreements.**
	Monitoring and Review of Supplier Services	10.2.1	Yes	In-Form Solutions monitors, reviews and audits vendor service delivery, where required.
	Managing Changes to Supplier Services	10.2.2	Yes	Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, is managed, taking into account of the criticality of business information systems and processes and re-assessment of risks.
12. Information Security Incident Management	**Management of Information Security Incidents and Improvements**	**11.1**	**Objective:**	**To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.**
	Responsibilities and Procedures	11.1.1	Yes	Management responsibilities and procedures are established to ensure a quick, effective, and orderly response to information security incidents.
	Reporting Information Security Events	11.1.2	Yes	We have procedures in place to ensure security events are reported and recorded. These procedures are supported with training courses and policy.
	Reporting Information Security Weaknesses	11.1.3	Yes	All employees, contractors and third-party users of information technology systems and services are required to report any observed or suspected weaknesses in information technology systems or services using the same mechanisms as for actual Security Events.
	Assessment of and Decision on Information Security Events	11.1.4	Yes	The assessment of incident security events and the decision to classify as an information security incident is defined in our policy and procedure.
	Response to Information Security incidents	11.1.5	Yes	The response to information security incidents are defined in policy and process documents.
	Learning from Information Security Incidents	11.1.6	Yes	We apply a learning and continual improvement approach to all information security incidents.
	Collection of Evidence	11.1.7	Yes	Policy and process set out the procedure for gathering and retaining evidence and the chain of custody.
13. Information Security Aspects of Business Continuity Management	**Information Security Continuity**	**12.1**	**Objective:**	**Information security continuity shall be embedded in the organisation's business continuity management systems.**
	Planning Information	12.1.1	Yes	A managed process has been developed and is maintained for business

	Security Continuity			continuity throughout In-Form Solutions including the UK and with relevant third-party vendors that addresses the information security requirements needed for the organisation's business continuity.
	Implementing Information Security Continuity	12.1.2	Yes	Plans have been developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required timescales following interruption to, of failure of, critical business processes. Events that cause interruptions to business processes are identified, along with the probability and impact of such interruptions and their consequences for information security.
	Verify, Review and Evaluate Information Security Continuity	12.1.3	Yes	Business Continuity Plans are tested and externally audited annually (ISO9001 & Cyber Essentials Plus) updated periodically to ensure that they are up to date and effective.
	Redundancies	**12.2**	**Objective:**	**To ensure availability of information processing facilities.**
	Availability of Information Processing Facilities	12.2.1	Yes	A managed process has been developed and maintained for establishing, documenting, implementing and maintaining processes, procedures and controls to ensure the required level of continuity for information security during an adverse, unplanned or emergency situation.
14. Compliance	**Compliance with Legal and Contractual Requirements**	**13.1**	**Objective:**	**To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.**
	Identification of Applicable Legislation and Contractual Obligations	13.1.1	Yes	Registers are maintained to capture relevant information security related statutory, regulatory and contractual obligations.
	Intellectual Property Rights (IPR)	13.1.2	Yes	Appropriate procedures are implemented to ensure compliance with statutory, regulatory, and other legal obligation requirements on the user of material in respect of which there may be intellectual property rights and on the use of proprietary software products.
	Protection of Records	13.1.3	Yes	Policies are in place to ensure records are protected from loss, destruction and falsification, in accordance with statutory and regulatory and other legal obligation and business requirements.
	Privacy and Protection of Personal Identifiable Information	13.1.4	Yes	Our Data Protection Policy and Privacy Policy, procedures and training support relevant statutory and regulatory and (if applicable) in other legal requirements.
	Information Security Reviews	**13.2**	**Objective:**	**To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.**

	Independent Review of Information Security	13.2.1	Yes	Audits are conducted internally and externally (annually Cyber Essentials Plus) by persons independent of the function of management being audited.
	Compliance with Security Policies and Procedures	13.2.2	Yes	Leaders are responsible for ensuring compliance within their areas of responsibility. Non-compliance, corrective action and opportunities for improvement are also reviewed at Management Review Meetings.
	Technical Compliance Review	13.2.3	Yes	Information technology systems are checked for compliance with security implementation standards.
Additional Controls	**Continual Improvement**	**D&B Control**	**Objective:**	**Continual Improvement**
	Learning from other organisations entities & driving improvements.	C01	Yes	In-Form Solutions regularly meet with professional advisers, are externally and internally audited by numerous professional organisations (ISO9001, Cyber Essentials Plus, NHS England Information Governance Toolkit) meet to share best practice, identify continual improvement opportunities and track changes.

This Statement of Applicability has been approved and authorised by:

Name: David Poynton

Position: Chairman

Date: 5th January 2024

Signature: