ibCom

ISO/IEC 27001
Statement of Applicability

ibCom management attest that following controls are in place in regards to risks relating to confidentiality, integrity and availability of customer data stored on the ibCom mydigitalstructure platform.

Mark Byers
Chief Risk Officer, October 2013

	Management direction for information security	
5.1.1	Policies for information security	Part of the employment contract.
5.1.2	Review of the policies for information security	Monthly review and re-distribution.
	Internal organization	
6.1.1	Information security roles and responsibilities	ibCom's Chief Risk Officer (CRO) controls all roles.
6.1.2	Segregation of duties	Only operational employees have access to data.
6.1.3	Contact with authorities	Responsibility of CRO.
6.1.4	Contact with special interest groups.	Responsibility of CRO.
6.1.5	Information security in project management	All projects relating to a potential change in the platform have information security as a first class citizen.
	Mobile devices & teleworking	
6.2.1	Mobile device policy	All access to AWS infrastructure on a mobile device is also protected via 2 factor authentication and/or IP address restrictions.

6.2.2	Teleworking	No data is stored at teleworking sites.
	Prior to employment	
7.1.1	Screening	As its first measure, ibCom uses very few employees that have access to customer data. To get access to customer data an employee must have a minimum of one (1) years experience with ibCom or an equivalent well proven service.
7.1.2	Terms and conditions of employment	Information security is at the heart of the ibCom employment contract - including post employment.
	During employment	
7.2.1	Management responsibilities	Any breach by an ibCom employee in regards to information security results in immediate termination.
7.2.2	Information security awareness, education & training	All employees will have appropriate industry qualifications or experience and are constantly made aware of information security policies - it is a core value of ibCom.
7.2.3	Disciplinary process	Any breach by an ibCom employee in regards to information security results in immediate termination.
	Termination & change of employment	
7.3.1	Termination of change of employment responsibilities	User access roles are effected immediately and employee obligations are re-communicated.
	Asset Management	
8.1.1	Inventory of assets	All core customer data management assets are managed contractually within AWS. All ibCom assets used to access AWS or other operational administrative services are registered and maintained.
8.1.2	Ownership of	All assets are owned by ibCom operations and the

	assets	CRO.
8.1.3	Acceptable use of assets	All ibCom assets are clearly identified and linked to the employees role.
8.1.4	Return of assets	Once an employee now longer has a role within ibCom, assets are automatically returned to the direct responsibility of the CRO.
	Information classification	
8.2.1	Classification of information	All information is classified based on zone: lab (private), operations (private) & engagement (public)
8.2.2	Labelling of information	*Documented*
8,2.3	Handling of assets	*Documented*
	Media handling	
8.3.1	Management of removable media	Removable media is not allowed on operational assets.
8.3.2	Disposal of media	*Not applicable*
8.3.3	Physical media transfer	*Not applicable*
	Business requirements of access control	
9.1.1	Access control policy	Information is controlled within AWS and mydigitalstructure using inherent access control functionality.
9.1.2	Access to networks & network services	All key information is stored in internet based secure stores, using encrypted access protocols - no measures needed to control this risk.
	User access management	

9.2.1	User registration & de-registration	Information is controlled within AWS and mydigitalstructure using inherent access control functionality.
9.2.2	User access provisioning	Provisioning can only be done by the directors of ibCom.
9.2.3	Management of privileged access rights	Privileged rights can only be assigned by the directors of ibCom.
9.2.4	Management of secret authentication information of users	Can only be done by the directors of ibCom.
9.2.5	Review of user access rights	Reviewed monthly.
9.2.6	Removal of adjustment of access rights	As soon as an employee's role is changed, so are their access rights. They are removed before the employee is notified.
	User responsibilities	
9.3.1	Use of secret authentication information	All employee's are aware of restrictions on the use of secret information.
	System & application access control	
9.4.1	Information access restriction	Controlled by AWS & mydigitalstructure access control functionality.
9.4.2	Secure log-on procedures	All information is protected by secure log-on procedures.
9.4.3	Password management system	All passwords have industry standard minimum lengths/strengths and 2nd factor is used.
9.4.4	Use of privileged utility	There are no privileged utility programs.

	programs	
9.4.5	Access control to program source code	All access to all source code is highly restricted.
	Cryptographic controls	
10.1.1	Policy on the user of cryptographic controls	*Documented*
10.1.2	Key management	*Documented*
	Secure areas	
11.1.1	Physical security perimeter	*Refer AWS security compliance*
11.1.2	Physical entry controls	*Refer AWS security compliance*
11.1.3	Securing offices, rooms & facilitates	*Refer AWS security compliance*
11.1.4	Protecting against external and environmental threats	*Refer AWS security compliance*
11.1.5	Working in secure areas	*Refer AWS security compliance*
11.1.6	Delivery & loading areas	*Refer AWS security compliance*
	Equipment	
11.2.1	Equipment siting & protection	*Refer AWS security compliance*

11.2.2	Supporting utilities	*Refer AWS security compliance*
11.2.3	Cabling security	*Refer AWS security compliance*
11.2.4	Equipment maintenance	*Refer AWS security compliance*
11.2.5	Removal of assets	*Refer AWS security compliance*
11.2.6	Security of equipment & assets off-premises	*Refer AWS security compliance*
11.2.7	Secure disposal or reuse of equipment	*Refer AWS security compliance*
11.2.8	Unattended user equipment	*Refer AWS security compliance*
11.2.9	Clear desk and clear screen policy	*Refer AWS security compliance*
	Operational procedures & responsibilities	
12.1.1	Documented operating procedures	*Documented*
12.1.2	Change management	All change management is tightly controlled.
12.1.3	Capacity management	ibCom uses the inherent scalability in AWS Infrastructure as a Service.
12.1.4	Separation of development, testing & operational environments.	The *lab* and *operational* zones are procedurally separated.
	Protection from malware	

12.2.1	Controls agains malware	All employees are aware of the issues associated with malware and scanning software is used.
	Backup	
12.3.1	Information backup	All information is backed up and restore procedures are constantly being tested.
	Logging & monitoring	
12.4.1	Event logging	All events/actions on information are logged and reviewed.
12.4.2	Protection of log information	All logs are secured.
12.4.3	Administrator & operator logs	*As per 12.4.1*
12.4.4	Clock synchronisation	All information is stored in a single time zone.
	Control of operational software	
12.5.1	Installation of software on operational systems	Instances are re-imaged once a well-proven instance has been fully tested.
	Technical vulnerability management	
12.6.1	Management of technical vulnerabilities	*Documented*
12.6.2	Restrictions on software installation	*Documented*
	Information systems audit considerations	
12.7.1	Information systems audit controls	All verification process are carefully controlled and use "mirror" images.
	Network security management	

13.1.1	Network controls	All networks are protected using firewalls. *Refer AWS security compliance*
13.1.2	Security of network services	*Refer AWS security compliance*
13.1.3	Segregation in networks	All ibCom zones (lab, operations, engagement) use isolated networks.
	Information transfer	
13.2.1	Information transfer policies & procedures	*Refer AWS security compliance*
13.2.2	Agreements on information transfer	All information is secured by encryption over the wire.
13.2.3	Electronic messaging	All highly sensitive information can be secure using theoperations@ibcom.biz PGP public key.
13.2.4	Confidentiality or non-disclosure agreements	Confidentiality and non-disclosure is default in any engagement with ibCom.
	Security requirements of information systems	
14.1.1	Information security requirements analysis & specification	*Documented*
14.1.2	Securing application services on public networks	*Documented*
14.1.3	Protecting application services transactions	All transactions are encrypted with SSL and DH based perfect forward security.

	Security in development & support processes	
14.2.1	Secure development policy	*Documented*
14.2.2	System change control procedures	*Documented.* Changes are minimal. There is a clear separation between the *lab* zone and the *operational* zone.
14.2.3	Technical review of applications after operating platform changes	*Documented*
14.2.4	Restrictions on changes to software	All changes are discouraged and strictly controlled.
14.2.5	Secure system engineering principles	Using of MVC and separation-of-concerns, combined with a "kernel" mode and "user" mode allow for security zoning,more...
14.2.6	Secure development environment	The development environment (lab zone) uses the same protocols as the production environment (operations zone).
14.2.7	Outsourced security testing	There is no outsourced development within the ibCom layer.
14.2.9	System acceptance testing	*Documented*
	Test data	
14.3.1	Protection of test data	Test data is protected under same protocols as production data.
	Information security in supplier relationships	
15.1.1	Information security policy for supplier	*Refer AWS security compliance*

	relationships	
15.1.2	Addressing security within supplier agreements	*Refer AWS security compliance*
15.1.3	Information & communication technology supply chain	*Documented and refer AWS security compliance*
	Supplier service delivery management	
15.2.1	Monitoring & review of supplier services	AWS is monitored constantly.
15.2.2	Managing changes to supplier services	Highly infrequent, if at all. Months of planning an risk analysis before any change is made.
	Management of information security incidents & improvements	
16.1.1	Responsibilities & procedures	*Documented*
16.1.2	Reporting information security events	Events are reported to all stake-holders as soon as they are known, including the @ibComMYDS twitter account andstatus.mydigitalstructure.com.
16.1.3	Reporting information security weakness	ibCom has a reward for report program. All highly sensitive information can be secure using the operations@ibcom.biz PGP public key.
16.1.4	Assessment of & decision on information security events	*Documented*
16.1.5	Response to information security	All incidents considered to be security incidents are immediately communicated to all effected stakeholders. Including the use

	incidents	of @ibComMYDS twitter account & status.mydigitalstructure.com.
16.1.6	Learning from information security incidents	All learnings from incidents are immediately applied to the platform.
16.1.7	Collection of evidence	*Documented*
	Information security continuity	
17.1.1	Planning information security continuity	ibCom has a full disaster plan - including running mirror instances in other geographical locations.
17.1.2	Implementing information security continuity	All mirror sites operate within the same production (operational zone) protocols.
17.1.3	Verify, review & evaluate information continuity	Verification, review & evaluation occurs constantly.
	Redundancies	
17.2.1	Availability of information processing facilities	Mirror sites are implemented in other geographical locations.
	Compliance with legal & contractual requirements	
18.1.1	Identification of applicable legislation & contractual requirements	*Documented*
18.1.2	Intellectual property rights	All software and information intellectual property rights are well known and managed.

18.1.3	Protection of records	All records are highly protected.
18.1.4	Privacy & protection of personally identifiable information	All private information is highly protected.
18.1.5	Regulation of cryptographic controls	*Documented*
	Information security reviews	
18.2.1	Independent review of information security	Third party certiification is underway *(as at December 2013)*
18.2.2	Compliance with security policies & standards	Constantly being reviewed for compliance.
18.2.3	Technical compliance review	Constantly being reviewed for compliance.

END