



Statement of Applicability

Document classification: Public

Internet Central Ltd
Innovation Centre
Keele Science Park
Keele
Staffordshire
ST5 5NB

Applicable for all services supplied by Internet Central Limited (IC)

tel 01782 667788
fax 01782 667799

Revision date 23/01/2018

The reason for inclusion of selected controls below were identified as an output from of our risk treatment plan devised as a result of our information security risk assessment.

Control	Description	Selected	Implemented
A.5.1.1	Policies for information security	Yes	Yes
A.5.1.2	Review of the policies for information security	Yes	Yes
A.6.1.1	Information security roles and responsibilities	Yes	Yes
A.6.1.2	Segregation of duties	Yes	Yes
A.6.1.3	Contact with authorities	Yes	Yes
A.6.1.4	Contact with special interest groups	Yes	Yes
A.6.1.5	Information security in project management	Yes	Yes
A.6.2.1	Mobile device policy	Yes	Yes
A.6.2.2	Teleworking	Yes	Yes
A.7.1.1	Screening	Yes	Yes
A.7.1.2	Terms and conditions of employment	Yes	Yes
A.7.2.1	Management responsibilities	Yes	Yes
A.7.2.2	Information security awareness, education and training	Yes	Yes
A.7.2.3	Disciplinary process	Yes	Yes
A.7.3.1	Termination or change of employment responsibilities	Yes	Yes
A.8.1.1	Inventory of assets	Yes	Yes
A.8.1.2	Ownership of assets	Yes	Yes

A.8.1.3	Acceptable use of assets	Yes	Yes
A.8.1.4	Return of assets	Yes	Yes
A.8.2.1	Classification of information	Yes	Yes
A.8.2.2	Labelling of information	Yes	Yes
A.8.2.3	Handling of assets	Yes	Yes
A.8.3.1	Management of removable media	Yes	Yes
A.8.3.2	Disposal of media	Yes	Yes
A.8.3.3	Physical media transfer	Yes	Yes
A.9.1.1	Access control policy	Yes	Yes
A.9.1.2	Access to networks and network services	Yes	Yes
A.9.2.1	User registration and de-registration	Yes	Yes
A.9.2.2	User access provisioning	Yes	Yes
A.9.2.3	Management of privileged access rights	Yes	Yes
A.9.2.4	Management of secret authentication information of users	Yes	Yes
A.9.2.5	Review of user access rights	Yes	Yes
A.9.2.6	Removal or adjustment of access rights	Yes	Yes
A.9.3.1	Use of secret authentication information	Yes	Yes
A.9.4.1	Information access restriction	Yes	Yes
A.9.4.2	Secure log-on procedures	Yes	Yes
A.9.4.3	Password management system	Yes	Yes
A.9.4.4	Use of privileged utility programs	Yes	Yes
A.9.4.5	Access control to program source code	Yes	Yes
A.10.1.1	Policy on the use of cryptographic controls	Yes	Yes
A.10.1.2	Key management	Yes	Yes
A.11.1.1	Physical security perimeter	Yes	Yes

A.11.1.2 Physical entry controls	Yes	Yes
A.11.1.3 Securing offices, rooms and facilities	Yes	Yes
A.11.1.4 Protecting against external and environmental threats	Yes	Yes
A.11.1.5 Working in secure areas	Yes	Yes
A.11.1.6 Delivery and loading areas	Yes	Yes
A.11.2.1 Equipment siting and protection	Yes	Yes
A.11.2.2 Supporting utilities	Yes	Yes
A.11.2.3 Cabling security	Yes	Yes
A.11.2.4 Equipment maintenance	Yes	Yes
A.11.2.5 Removal of assets	Yes	Yes
A.11.2.6 Security of equipment and assets off-premises	Yes	Yes
A.11.2.7 Secure disposal or re-use of equipment	Yes	Yes
A.11.2.8 Unattended user equipment	Yes	Yes
A.11.2.9 Clear desk and clear screen policy	Yes	Yes
A.12.1.1 Documented operating procedures	Yes	Yes
A.12.1.2 Change management	Yes	Yes
A.12.1.3 Capacity management	Yes	Yes
A.12.1.4 Separation of development, testing and operational environments	Yes	Yes
A.12.2.1 Controls against malware	Yes	Yes
A.12.3.1 Information backup	Yes	Yes
A.12.4.1 Event logging	Yes	Yes
A.12.4.2 Protection of log information	Yes	Yes
A.12.4.3 Administrator and operator logs	Yes	Yes
A.12.4.4 Clock synchronisation	Yes	Yes
A.12.5.1 Installation of software on operational systems	Yes	Yes

A.12.6.1 Management of technical vulnerabilities	Yes	Yes
A.12.6.2 Restrictions on software installation	Yes	Yes
A.12.7.1 Information systems audit controls	Yes	Yes
A.13.1.1 Network controls	Yes	Yes
A.13.1.2 Security of network services	Yes	Yes
A.13.1.3 Segregation in networks	Yes	Yes
A.13.2.1 Information transfer policies and procedures	Yes	Yes
A.13.2.2 Agreements on information transfer	Yes	Yes
A.13.2.3 Electronic messaging	Yes	Yes
A.13.2.4 Confidentiality or non-disclosure agreements	Yes	Yes
A.14.1.1 Information security requirements analysis and specification	Yes	Yes
A.14.1.2 Securing application services on public networks	Yes	Yes
A.14.1.3 Protecting application services transactions	Yes	Yes
A.14.2.1 Secure development policy	Yes	Yes
A.14.2.2 System change control procedures	Yes	Yes
A.14.2.3 Technical review of applications after operating platform changes	Yes	Yes
A.14.2.4 Restrictions on changes to software packages	Yes	Yes
A.14.2.5 Secure system engineering principles	Yes	Yes
A.14.2.6 Secure development environment	Yes	Yes
A.14.2.7 Outsourced development	Yes	Yes
A.14.2.8 System security testing	Yes	Yes
A.14.2.9 System acceptance testing	Yes	Yes
A.14.3.1 Protection of test data	Yes	Yes
A.15.1.1 Information security policy for supplier relationships	Yes	Yes
A.15.1.2 Addressing security within supplier agreements	Yes	Yes

A.15.1.3 Information and communication technology supply chain	Yes	Yes
A.15.2.1 Monitoring and review of supplier services	Yes	Yes
A.15.2.2 Managing changes to supplier services	Yes	Yes
A.16.1.1 Responsibilities and procedures	Yes	Yes
A.16.1.2 Reporting information security events	Yes	Yes
A.16.1.3 Reporting information security weaknesses	Yes	Yes
A.16.1.4 Assessment of and decision on information security events	Yes	Yes
A.16.1.5 Response to information security incidents	Yes	Yes
A.16.1.6 Learning from information security incidents	Yes	Yes
A.16.1.7 Collection of evidence	Yes	Yes
A.17.1.1 Planning information security continuity	Yes	Yes
A.17.1.2 Implementing information security continuity	Yes	Yes
A.17.1.3 Verify, review and evaluate information security continuity	Yes	Yes
A.17.2.1 Availability of information processing facilities	Yes	Yes
A.18.1.1 Identification of applicable legislation and contractual requirements	Yes	Yes
A.18.1.2 Intellectual property rights	Yes	Yes
A.18.1.3 Protection of records	Yes	Yes
A.18.1.4 Privacy and protection of personally identifiable information	Yes	Yes
A.18.1.5 Regulation of cryptographic controls	Yes	Yes
A.18.2.1 Independent review of information security	Yes	Yes
A.18.2.2 Compliance with security policies and standards	Yes	Yes
A.18.2.3 Technical compliance review	Yes	Yes