iomart

Following the

NCSC Cloud Security Principles

Information Security Management

February 2017

GRC

Governance | Risk | Compliance

National Cyber Security Centre

a part of GCHQ

Important Information

This document is for information only and has been prepared as guidance.

Every effort has been made to ensure the accuracy of all information contained in this document; it may include typographical errors.

Please ask questions if any part of this document is not clear.

Compliance Department | Lister Pavilion, West of Scotland Science Park, Glasgow, G20 0SP | email: compliance@iomart.com | Tel: +44 (0)141 931 6400

Introduction

This information document provides information on how iomart associates its cloud hosting services with the National Cyber Security Centre (NCSC) Cloud Security Principles and the objectives of these principles as part of NCSC's Cloud Security Guidance

The intention of this document is to provide background information for business users using iomart cloud hosting services using classified data with the protective markings up to OFFICIAL or OFFICIAL–SENSITIVE as described in the United Kingdom (UK) Government Security Classification Policy (GSCP) and describes how iomart manages OFFICIAL information to adhere with the NCSC Cloud Security Principles.

This document describes:

- What security processes iomart have implemented to adhere to each of the Cloud Security Principles
- How iomart is managing and securing content stored on iomart hosted cloud services.
- How iomart hosted cloud services operate and risk approach.

This document will allow iomart customers and business users (the 'user') to make informed decisions when performing risk assessments to help address common security requirements as described in the NCSC Cloud Security Principles

Context

HM Government information assets are currently classified into three categories: OFFICIAL, SECRET and TOP SECRET. Each information asset classification attracts a baseline set of security controls providing appropriate protection against typical threats.

The legacy Impact Level accreditation scheme has been phased out and is no longer the mechanism used to describe the security properties of a system, including cloud services. Public sector organisations are ultimately responsible for risk management decisions relating to the use of cloud services.

Further guidance should always be sought from the business Senior Information Risk Owner (SIRO) or from an appropriate compliance adviser in relation to data privacy and security requirements, including applicable laws or requirements.

Shared Responsibility

With a managed cloud hosting service from iomart there is a shared responsibility between the user and iomart.

Users should carefully consider the services they choose from iomart, as their responsibilities vary depending on the services they use, the integration of those services into their IT environments, and applicable laws and regulations.

Typically, iomart operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate with the user assuming responsibility for and management of any associated application software (including updates and security patches).

Cloud Security Principles

The NCSC Cloud Security Guidance lists 14 essential principles to consider when evaluating cloud services, and why these are important to public sector organisation.

Users are required to decide which of the principles are important to their business, and how much (if any) assurance is required in the implementation of these principles.

Below iomart has outlined how they adhere to each of the 14 Cloud Security Principles and the related assurance approach.

Principle 1	Data in Transit Protection	**Requirement** User data transiting networks should be adequately protected against tampering and eavesdropping via a combination of network protection and encryption. **How does iomart adhere?** Mechanisms are in place to restrict unauthorized internal and external access to data with access to data appropriately segregated. Firewalls configured not to permit traffic from a source IP or Media Access Control (MAC) address other than its own Service supports both IPsec and TLS for protection of data in transit. Data in transit protection for iomart services are subject to audit at least annually under ISO 27001 and PCI-DSS certification requirements. UK Gov Cabinet Office PSN Connections and Service Provision Compliant
Principle 2	Asset Protection and Resilience	**Requirement** User data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure. **How does iomart adhere?** All iomart UK data centres are suitable for all data classified at OFFICIAL, including OFFICIAL-SENSITIVE data under the GSCP UK Sovereign cloud platform delivered from TEN secure UK data centres by a UK company with SC and DV cleared UK staff Data centres are accredited to ISO9001 and ISO27001 with ISO 27017 codes of practice for information security controls on cloud services and 27018 for the protection of Personally Identifiable Information in the cloud incorporated. Only approved employees and contractors who have a legitimate business need have physical access to iomart data centres. Access privileges are reviewed quarterly, should a role change occur access is revoked, even if the person continue to be an employee. Access is automatically revoked when an employee leaves iomart. External and internal security is managed by iomart employees utilising video surveillance, intrusion detection systems and other electronic means Physical access is controlled using multi-factor authentication mechanisms to access data halls. Encryption used as applicable and on request to protect data at rest Industry best practice is used to ensure that data storage devices are erased when resources are moved, re-provisioned, when leave service or on request. Data storage devices that have reached the end of life are degaussed and physically destroyed in accordance with industry best practice i.e. NIST 800-88 (“Guidelines for Media Sanitization”).

Principle

3

Separation between Users

Requirement

Separation should exist between different Users of the service to prevent one malicious or compromised User from affecting the service or data of another.

How does iomart adhere?

Each tenant's servers are segregated into their own VLAN

iomart consult with clients to determine if servers need configured to further split server farms over separate security zones. This ensures that uncontrolled network communications do not occur through adjacent architectural tiers

Storage presentation is segregated through the use of fibre-channel zoning, prohibiting any host from accessing unauthorised storage areas

By default, network security is set to deny all network traffic in all directions. iomart will consult with clients to determine the most appropriate firewall configuration, enabling access to ports as required

Principle

4

Governance Framework

Requirement

The service provider should have a security governance framework that coordinates and directs their overall approach to the management of the service and information within it.

How does iomart adhere?

Our Cloud services have the appropriate management and security governance controls in place.

PSN connection and service certification for Private Cloud, Private Community Cloud or Public Cloud verified by a IA Architect from NCSC

Certified Information Security Management System to ISO27001:2013 using on ISO 27002 controls with iomart's security roles established and incorporating ISO 27017 codes of practice for information security controls on cloud services and 27018 for the protection of Personally Identifiable Information in the cloud.

Forms part of the iomart Group Integrated Management System

Principle

5

Operational Security

Requirement

The service provider should have processes and procedures in place to ensure the operational security of the service.

How does iomart adhere?

iomart operate fully mature and robust processes in line with the ISO27001 standard.

The following controls are in place:

- Change Management process to prevent unintended service disruptions and maintain the integrity of the service.
- Vulnerability Management to oversee iomart (not user) internet facing services with scans of all endpoint IP addresses for vulnerabilities and external threat assessments performed regularly by an independent security firm.
- Protective Monitoring for key iomart operational systems and services with security metrics defined and alarms configured to automatically notify operations and management 24x7x365 when early warning thresholds are crossed including denial of service attacks.
- Incident Management process implemented with a formal, documented incident response procedures and program, addressing purpose, roles, responsibilities, and management commitment.

Principle 6	Personnel Security	Requirement Service provider staff should be subject to personnel security screening and security education for their role. How does iomart adhere? iomart use the Baseline Personnel Security Standard (BPSS) as a base line for checking employment status with security checks before employing staff and contractors with access to data Senior administrators or people who have access to sensitive data are required to go through a Security Check (SC) and others go through Developed Vetting (DV) iomart ensure that information security responsibilities are included in terms and conditions of employment iomart provide security education, training and awareness to all staff commensurate with their role iomart ensure that all access rights and permissions assigned to users are revoked on termination of their employment. The revocation of access rights and permissions is included in the employment termination process
Principle 7	Secure Development	Requirement Services should be designed and developed to identify and mitigate threats to their security. How does iomart adhere? Follows best practice in accordance with ISO 27001 certification standards, Iomart software development process encompasses formal design reviews, threat modelling, and completion of a risk assessment with recurring penetration testing performed by recognised industry experts. Certification from the UK Gov Cabinet Office to connect iomart's infrastructure, cloud and backup services to the Public Services Network (PSN) meeting requirements for PSN Connection and Service Compliance, Incorporated controls from ISO 27017 codes of practice for information security controls on cloud services and 27018 for the protection of Personally Identifiable Information in the cloud.
Principle 8	Supply Chain Security	Requirement The service provider should ensure that its supply chain satisfactorily supports all of the security principles that the service claims to implement. How does iomart adhere? Supply chain and procurement managed in accordance with ISO 9001, ISO 27001, and ISO 20000 management systems obligations and subject to audit at least annually. The iomart supplier evaluation procedure ensures that appropriate sub-contractors are evaluated, assessed and appointed in line with business requirements. iomart operates a procedure for the evaluation of the information security arrangements of our suppliers and sub-contractors so that a degree of confidence may be gained that they have implemented sufficient controls to support iomart requirements. Personnel security requirements for suppliers supporting iomart services are established in a Mutual Non-Disclosure Agreement.

Principle

9

Secure User Management

Requirement

Users should be provided with the tools required to help them securely manage their service.

How does iomart adhere?

Users are provided with access to their services through a secure management portal and control panel

All managed systems are monitored, access is logged and tracked for auditing purposes

Passwords associated with remote management access are a minimum of 7 characters, alphanumeric and changed every 90 days. Passwords are not reused within 20 changes. All passwords PGP encrypted

Principle

10

Identity and Authentication

Requirement

Access to all service interfaces (for Users and providers) should be constrained to authenticated and authorised individuals.

How does iomart adhere?

Remote management access is on a need to know basis

Remote management access is authenticated and directly associated to authorised individuals rather than group accounts

All managed systems monitored and access logged and tracked for auditing purposes

Passwords associated with remote management access are a minimum of 7 characters, alphanumeric and changed every 90 days. Passwords are not reused within 20 changes. All passwords PGP encrypted

All employees with management access to platforms advised of any custom or specific security operating procedures and activities governing its use

Principle

11

External Interface Protection

Requirement

All external or less trusted interfaces of the service should be identified and have appropriate protections to defend against attacks through them.

How does iomart adhere?

Protecting the confidentiality, integrity, and availability of systems and data is paramount in order to ensure user trust and confidence.

The iomart control panel has been architected to permit users to select the level of security appropriate for an authorised person and is carefully monitored and managed.

By default, network security is set to deny all network traffic in all directions. iomart will consult with clients to determine the most appropriate firewall configuration, enabling access to ports as required

Principle 12	Secure Service Administration	Requirement The methods used by the service provider's administrators to manage the operational service should be designed to mitigate any risk of exploitation that could undermine the security of the service. How does iomart adhere? Access to systems is role specific with user accounts created on justification and approval owner or manager. Access changed on moving role and disabled immediately on leaving role with access requirements reviewed regularly. Passwords changes required every 60 days Password complexity for user authentication managed is in accordance with iomarts integrated management system password policy. Systems Administrators are required to use multifactor authentication to gain access to systems they maintain. Secure service administration and related processes are subject to audit at least annually under ISO 27001 and PCI-DSS requirements
Principle 13	Audit Information for users	Requirement Users should be provided with the audit records they need to monitor access to their service and the data held within it. How does iomart adhere? Users systems are monitored in accordance with service requirements and access logged and tracked for auditing purposes and available through the user secure management portal and control panel iomart systems are regularly audited by independent verifying bodies for compliance with numerous international standards (ISO) by a UKAS accredited certifying body as well as other industry bodies like PCI DSS and for adherence with PSN, NCSC, NHS N3 and PASF requirements.
Principle 14	Secure Use of the Service	Requirement Users have certain responsibilities when using a cloud service in order for this use to remain secure, and for their data to be adequately protected. How does iomart adhere? iomart have a user Acceptable Use Policy that provides guidance and informs users on acceptable use of iomart services. This policy includes guidance on illegal, harmful, or offensive content, security violations, network abuse and e-mail or message abuse with information on monitoring and enforcement of the policy. The user secure management portal and control panel allows to be notified of operational issues that impact the user service with a unique ticket generated for reference In accordance with service requirements iomart provide account management and support to identify common security misconfigurations, suggestions for improving system performance, and underutilized resources.