Ideagen Information Security Overview

INFOSEC-0107 | Revision 2

Ideagen

Contents

Ideagen Limited T: +44 1629 699 100 e: info@ideagen.com w: www.ideagen.com

CLASSIFIED AS PUBLIC

Ideagen Limited T: +44 1629 699 100 e: info@ideagen.com w: www.ideagen.com

Ideagen Security Practices

This document identifies the security practices that Ideagen organisations performing software services, including Ideagen's customer support and software products provided as a service, follow when performing such services ("services") under the terms of our MSSA, SLA and the Scope of Work/Order document or another contractual agreement we enter into (collectively the "order"). It also clarifies your security obligations with respect to your environments and the data therein. These practices are subject to change at Ideagen's discretion; however, Ideagen will not materially reduce the level of security specified in this document during the performance of services under your order.

Definitions

The term "environment(s)" means your technology environments to which Ideagen is granted access in order to provide the services and external environments where we provide hosting services and software provided as a service. The term "subcontractors" means subcontractors retained by Ideagen and its subsidiaries that assist in performing the services, such as Amazon Web Services (AWS), Azure etc.

Corporate Security Policies

Ideagen's corporate security policies cover the management of security for both its internal operations as well as the services Ideagen provides to its customers, and apply to all Ideagen employees as well as any applicable third parties and stakeholders. These policies, which are aligned with the ISO/IEC 27001:2013 standard to which Ideagen are externally certified, govern all areas of security applicable to the services.

Note that you are strongly encouraged to implement your own comprehensive system of policies, standards and procedures, according to your risk-based assessments and business requirements.

Ideagen's corporate security policies are confidential information and are not available for review by customers or third parties. However, brief summaries of certain security policies relevant to the provision of the services are provided below.

Organisational Security

The Ideagen ***Information Security Policy*** sets out Ideagen's approach to managing our information security objectives, and describes the principles for development, executive approval, implementation, and maintenance of all information security policies and practices at Ideagen. This over-arching information security policy also describes governing principles such as 'need to know', least privilege, and segregation of duties. This Policy is defined and approved by management and communicated to all employees (permanent and temporary) and relevant external parties, who are subject to all Ideagen securitypolicies. This Ideagen ***Information Security Policy*** is supported by the following topic-specific policies, which further mandate the implementation of information security controls:

Access Control

The Ideagen ***Access Control Policy*** describes logical access control requirements for all Ideagen systems, including authentication, authorisation, access approval, provisioning, and revocation for employees and any other Ideagen-defined 'users' with access to Ideagen systems.

Information Classification and Handling

The Ideagen ***Information & Asset Classification, Labelling and Handling Procedure*** provides guidelines for all Ideagen personnel regarding information classification schemes and minimum handling requirements

Ideagen Limited T: +44 1629 699 100 e: info@ideagen.com w: www.ideagen.com

associated with those classifications. This ensures that all information receives an appropriate level of protection in accordance with its importance. For the avoidance of doubt, all customer-related information is assigned the highest level of classification.

The Ideagen *IT Asset Management Policy* details how Ideagen documents, risk assesses, classifies, handles, maintains and disposes of all assets, and which levels of security and controls are applicable to each.

The Ideagen *Risk Management Policy* details the processes and procedures involved in performing continual risk assessments against all information assets, and how we continually implement and monitor the effectiveness of all associated controls.

Physical and Environmental Security

The Ideagen *Physical and Environmental Security Policy* describes how Ideagen design, develop and implement security for our locations, systems, products and environments to prevent unauthorised physical access, damage and interference to Ideagen and information and information processing facilities and systems, as well as customer information.

End User Security

The Ideagen *IT Acceptable Use Policy* sets requirements for use of the Ideagen corporate network, computer systems, telephony systems, messaging technologies, Internet access, and other company resource.

Backup

The Ideagen *Backup Policy* details how Ideagen protect against loss of Ideagen or customer data, by implementing systems, controls and routines which ensure that all key information is regularly backed up in the applicable onsite or offsite locations, and tested on an ongoing basis to ensure effective and full recovery of the information is available.

Information Transfer

The Information Transfer section of the *Communications and Network Security Policy* details how Ideagen maintain the security of information transferred within our organisation and with any external entity. It describes the various controls, tools and security measures we have in place to ensure that the information is always secure, whether at rest or in transit, including measures which are in place to ensure that any information transmitted via any of our customer solutions, is secure.

Protection from Malware

The Ideagen *Antivirus and Malware Policy* details how Ideagen ensures that information and information processing facilities are protected against malware. It describes how we implement anti-virus tools and firewalls, as well as how we manage system and software updates and patches.

Computer Virus Controls

Ideagen maintains the following computer virus controls for computers issued to Ideagen employees:

- Ideagen maintains a mechanism within the Ideagen network that scans all email sent both to and from any Ideagen recipient for malicious code and deletes email attachments that are infected with known malicious code prior to delivery.
- Ideagen requires all Ideagen employee laptops to be loaded with virus protection software. Ideagen maintains mechanisms to ensure that virus definitions are regularly updated, and that updated definitions are published and communicated to employees. These mechanisms also give employees the ability to download new definitions and update virus protection software automatically. From time to time, Ideagen Global Cyber Security will conduct compliance reviews to ensure employees have the virus software installed and up to date virus definitions on all desktops and laptops.
- Information Security Managers: Ideagen have appointed an Information Security Manager as well as a third party Security Operations Centre (SOC) who serve as a resource to help identify strategic and practical security issues within the organisation. They serve as advocates within Ideagen to communicate information security awareness to Ideagen employees and management and work collectively with that group to help implement and comply with Ideagen's corporate security practices, policies and initiatives.

Management of Technical Vulnerabilities

Vulnerabilities are reviewed, risk ranked based on mitigations, environments etc, and then assigned to the responsible team for remediation in accordance with their classification.

Cryptographic Controls

The Ideagen *Cryptographic Controls Policy* details how Ideagen ensures proper and effective use of cryptography to protect the confidentiality, authenticity and integrity of information at all times. It details how we develop, implement and monitor a cryptographic controls policy and how we implement key management techniques to ensure that information is secure, and access to it, is restricted.

Communications and Network Security

The Ideagen *Communications and Network Security Policy* details how Ideagen ensures correct and secure operations of information processing facilities, how we record events and generate evidence, how we ensure the integrity of operational systems, how we minimise the impact of audit activities on operational systems, how we ensure the protection of information in networks and products and its supporting information processing facilities, how we ensure that information security is an integral part of information systems across the entire lifecycle, how we ensure that information security is designed and implemented within the development lifecycle of information systems and products and how we ensure the protection of data used for testing.

Privacy and Protection of Personally Identifiable Information

The *Data Protection Policy* and the *Privacy Policy* provides information on how Ideagen protects personal data. There are processes in place for responding to data subject requests and also for Data Protection Impact assessments, Legitimate Impacts Assessments and other privacy processes that supports the business activity.

Supplier Management

The Ideagen Suppliers and External Providers Management Policy describes how Ideagen ensure that information assets owned by all stakeholders (including customers) which are accessed by suppliers, are protected at all times.

Human Resource Security

The Ideagen ***General Rules and Code of Conduct Policy*** sets forth Ideagen's high standards for ethics and business conduct at every level of the company, and at every location where Ideagen does business throughout the world. The standards apply to employees, independent contractors, and temporary employees and cover the areas of legal and regulatory compliance and business conduct and relationships.

Incident Management

The Ideagen ***Incident Management Policy*** details how Ideagen ensures a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses. This includes responsibilities for internal communication, as well as responsibilities for communication with all applicable stakeholders, including customers and suppliers.

It requires reporting of and response to information security incidents in a timely and efficient manner. Ideagen also maintains a detailed Incident Response Plan to provide specific guidance for personnel involved in or supporting incident response.

Media Handling

The ***Media Handling Policy*** establishes guidelines for secure configuration, handling and erasure of information, from all types of electronic media, where use for current purposes is no longer needed and a decision has to be made regarding recycling or destruction. The policy is intended to protect Ideagen resources and information from security threats associated with the retrieval and recovery of information on electronic media.

Business Continuity and Disaster Recovery Management

The ***Business Continuity and Disaster Recovery (BCDR) Policy*** details how Ideagen determines our requirements for the continuity of information security management in adverse situations

The Ideagen Business Continuity Management process addresses the requirements for the development, maintenance and testing of emergency response, disaster recovery, and business continuity practices to minimize the impact of business disruptive events on Ideagen's internal business operations globally.

Compliance Management

The ***Compliance Management Policy*** details how Ideagen has implemented controls to avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any information security requirements. This includes how Ideagen ensures that information security is implemented and operated in accordance with Ideagen's policies and procedures.

Upon joining Ideagen, as part of their induction programme we provide employees with training on their role-specific duties as well as information and data security, quality and relevant areas of compliance, industry standards and legislation. We also schedule regular refresher training sessions to ensure that awareness remains at the required and expected levels.

Data Management/Protection for SaaS and Hosted Services

The following sections provide a summary of the key controls that have been implemented in accordance with the policies above in relation to the services provided.

Suppliers

Ideagen uses 3rd party organisations to provide the core infrastructure services as the foundation to the SaaS and hosted services provided to our customers. These organisations specialise in providing reliable and secure infrastructure to thousands of global, multi-national organisations.

They are very experienced, highly respected, and extremely compliant with all applicable regulations and legislation and have a comprehensive suite of materials and resources attesting to their various certifications, accreditations and memberships.

Prior to on boarding any SaaS and hosting services provider, we perform comprehensive diligence activities to ensure that they meet several critical minimum business requirements including but not limited to their financial stability, reputation, experience, ISO certifications and compliance with relevant regulations and legislation (applicable to the global location where data resides), security infrastructure and controls, capacity and resilience and continuity.

We perform ongoing assessments of these critical suppliers to ensure that they continue to provide the expected levels of service and security, and perform formally documented annual reviews, during which time we assess any issues, events or weaknesses which have been identified or notified, as well as obtaining up-to-date copies of their certifications, such as ISO/IEC 27001:2013 and SOC1, SOC2 and SOC3 compliance.

Physical Security

Ideagen utilises ISO/IEC 27001:2013 certified data centres that implement many controls to ensure the physical security of their customer's data.

Data centres are housed in nondescript facilities, and critical facilities have extensive setback and military grade perimeter control berms as well as other natural boundary protection. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilising video surveillance, state of the art intrusion detection systems, and other electronic means.

Authorised staff must pass two-factor authentication to access data centre floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorised staff. Data centre access and information is only provided to employees who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of the organisation. All physical and electronic access to data centres by employees is logged and audited routinely.

Environmental Safeguards

Fire Detection and Suppression

Automatic fire detection and suppression equipment has been installed to reduce risk. The fire detection system utilizes smoke detection sensors in all data centre environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems.

Power

The data centre electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centres use generators to provide backup power for the entire facility.

Climate and Temperature Control

Climate control is required to maintain a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages. Data centres are conditioned to maintain atmospheric conditions at optimal levels. Monitoring systems and data centre personnel ensure temperature and humidity are at the appropriate levels.

Management

Data centre staff monitor electrical, mechanical and life support systems and equipment so issues are immediately identified. Preventative maintenance is performed to maintain the continued operability of equipment.

Network Security

Ideagen takes the following steps to ensure secure operation of customer environments:

Firewalls

Firewalls are utilized to restrict access to systems from external networks and between systems internally. By default, all access is denied and only explicitly allowed ports and protocols are allowed based on business need. Each system is assigned to a firewall security group based on the system's function. Security groups restrict access to only the ports and protocols required for a system's specific function to mitigate risk.

DDoS Mitigation

Our infrastructure provides DDoS mitigation techniques including TCP Syn cookies and connection rate limiting in addition to maintaining multiple backbone connections and internal bandwidth capacity that exceeds the Internet carrier supplied bandwidth. We work closely with our providers to quickly respond to events and enable advanced DDoS mitigation controls when needed.

Spoofing and Sniffing Protections

Managed firewalls prevent IP, MAC, and ARP spoofing on the network and between virtual hosts to ensure spoofing is not possible. Packet sniffing is prevented by infrastructure including the hypervisor which will not deliver traffic to an interface which it is not addressed to. Ideagen utilises application isolation, operating system restrictions, and encrypted connections to further ensure risk is mitigated at all levels.

Port Scanning

Port scanning is prohibited and every reported instance is investigated by our infrastructure provider. When port scans are detected, they are stopped and access is blocked.

Data Management

During the performance of the services, you maintain control over and responsibility for any data residing in the environments. Ideagen does not and will not:

- Change any data, other than as required for the performance of the services.
- Have any role in determining or maintaining the accuracy of any data.
- Control how data is hosted, processed, stored or destroyed by you.
- Control your access to data, other than restricting access to data through applying physical and logical access controls, as applicable, as part of the services.
- Monitor your use of or access to data, except as necessary to provide the services.
- Take backup copies of your data other than to comply with Ideagen's service DR policies.

Deletion and/or return of Data

The deletion and/or return of customer data is covered under the MSSA and/or Data Processing Agreement (DPA).

Reporting Breaches

If the order specifies that Ideagen is required to access a production environment to perform the services and/or to receive production data into a development or test environment to perform the services, Ideagen will take the following additional measures:

- Ideagen will promptly evaluate and respond to incidents that create suspicions of unauthorised misappropriation of your data. Depending upon the nature of the activity, we will define escalation paths and response teams to address the incidents.
- If Ideagen determines that data in your environments has been misappropriated (including by an Ideagen employee), Ideagen will promptly report such misappropriation to you in writing, and will comply with the relevant data protection laws.
- Ideagen infrastructure staff and Ideagen personnel are instructed in addressing incidents where handling of data has been misappropriated, including prompt and reasonable reporting and escalation procedures.

Data Processing

Ideagen has implemented procedures designed to ensure that customer data is processed only as instructed by the customer, throughout the entire chain of processing activities by sub-processors. In particular, Ideagen and its affiliates have entered into written agreements with their sub-processors containing privacy, data protection and data security obligations that provide a level of protection appropriate to their processing activities. Compliance with such obligations as well as the technical and organizational data security measures implemented by Ideagen and its sub-processors are subject to regular formal documented reviews.

Data Encryption

The Services use industry-accepted encryption products to protect Customer Data and communications during transmissions between a customer's network and the Services, including 128-bit TLS 1.2 or higher Certificates and 2048-bit RSA public keys at a minimum with 4096-bit keys being preferred. Additionally, Customer Data is encrypted during transmission between data centres for replication / DR purposes. Data is encrypted at rest using the industry-standard AES-256 algorithm.

Reliability and Backup

All networking components, network accelerators, load balancers, web servers and application servers are configured in a redundant configuration. All Customer Data submitted to the Services is persisted on highly available and durable storage.

Depending on the service provided, all Customer Data submitted to the Services is automatically replicated on a near real-time basis to the secondary sites and is backed up on a regular basis and stored on backup media for a minimum of 7 days in production environments, after which it is securely overwritten or deleted. Any backups are verified for integrity and stored in the same geographical location as their instance.

Disaster Recovery

Ideagen has disaster recovery plans in place and tests them at least once per year. The Services utilise secondary facilities, along with required hardware, software, and Internet connectivity, in the event production facilities at the primary data centres were to be rendered unavailable.

The Services' disaster recovery plans currently have the following target recovery objectives: (a) restoration of the Service within 12 hours after Ideagen's declaration of a disaster; and (b) maximum Customer Data loss of 24 hours; excluding, however, a disaster or multiple disasters causing the compromise of both data centres at the same time, and excluding development and test bed environments.

Disclosure of Data

Ideagen will not disclose data located on Ideagen systems, including text and images, except in accordance with your order, your instructions, or to the extent required by law. Ideagen will use diligent efforts to inform you, to the extent permitted by law, of any request for such disclosure before disclosure is made.

Audit

In the event that the applicable order for services provides you with the right to audit Ideagen's compliance with these security practices, the following procedures apply. You may send Ideagen's a written request, including a detailed audit plan, at least four weeks in advance of the proposed audit date. The parties will work cooperatively to agree on a final audit plan. The audit shall be conducted no more than once during a twelve-month period, during regular business hours, subject to on-site policies and regulations, and may not unreasonably interfere with business activities. If you would like to use a third party to conduct the audit, the third-party auditor shall be mutually agreed to by the parties and the third-party auditor must execute a written confidentiality agreement acceptable to Ideagen. Upon completion of the audit, you will provide Ideagen with a copy of the audit report, which is classified as confidential information under the terms of the Agreement.

Access Control

Account Provisioning and Passwords

Ideagen maintains the following standards for provisioning access to and creating passwords for the environments that are in the control of Ideagen:

- Access is provisioned on a need to know and least privilege basis and enforcing segregation of duties where possible.
- Passwords conform to the strong password guidelines that include complexity, expiration, duplicity and length. Passwords shall not be written down or stored on-line unencrypted.
- Passwords are treated as Ideagen confidential information.
- User IDs and passwords to systems are not communicated to any other person without prior authorisation.

General Access

In the event of employee terminations, deaths or resignations, Ideagen will take actions to terminate network, telephony and physical access for such former employees. Ideagen Security Operations will periodically review accounts of terminated employees to verify that access has been terminated and that stale accounts are removed from the Ideagen network.

Human Resources Security

For all employees joining Ideagen, to ensure that they possess the required experience, skills, qualifications and "legal right to work" requirements, we perform various pre-employment screening checks.

Certain roles whereby employees have access to customer environment (systems, data, etc.) will be subject to specific additional screening checks when an offer of employment is made.

The additional checks include:

- Personal and professional references covering the last 2 years taken;
- Interviews with at least 2 different stakeholders.

Personnel

All Ideagen employees, independent contractors, and temporary employees are required to abide by the Ideagen General Rules and Code of Conduct.

Ideagen places strong emphasis on reducing risks of human error, theft, fraud, and misuse of facilities. Ideagen's efforts include personnel screening, making personnel aware of security policies, and training employees to implement security policies. For example, employees are expected to have a clear understanding of password policies and policies concerning the handling of confidential documentation.

Employee Security Requirements

Ideagen employees are required to take various measures to protect the security of the environments. Employee obligations include agreeing to confidentiality within the terms and conditions of their contract and compliance with company policies concerning protection of confidential information (e.g., Ideagen code of conduct, acceptable use and information protection policies). Employees also are required to take the following measures to protect your data:

- Store materials containing data securely and share those materials internally only for the purposes of providing the services.
- Dispose of paper copies of confidential materials and materials containing data in shredding bins designated for confidential information, and not in non-secure recycling bins or trashcans (if shredders are available at client site).

Your Obligations

You are responsible for all aspects of the collection of data, including determining and controlling the scope and purpose of collection. If you provide any personally identifiable information to Ideagen for use in the performance of the services, you are responsible for sending any required notices and/or obtaining any required consents necessary for Ideagen to perform the services. Ideagen does not and will not collect data from data subjects or communicate with data subjects about their data.

Where applicable you will limit Ideagen's access to your data to the extent necessary for Ideagen to perform the services. You will prevent Ideagen from accessing any health, payment card or other sensitive data that requires protections greater than those identified herein unless the parties specify the security measures applicable to Ideagen's treatment of such data in the applicable order for services.

Where applicable you are responsible for managing Ideagen's access to your systems, including providing unique accounts and user IDs where necessary.

END OF DOCUMENT

Ideagen Limited T: +44 1629 699 100 e: info@ideagen.com w: www.ideagen.com