iVvy.

Security Whitepaper

Contents

Induction

iVvy understands that the confidentiality, integrity and availability of our customers' data is vital to their business operations and, as a result, security is an integral part of iVvy's cloud computing applications, as well as a core element of iVvy's development processes. This document will outline how the iVvy platform and infrastructure secures its customers' data and is correct at the time of writing.

Overview

iVvy's security policy is designed to protect all of our clients' data by constantly monitoring and improving our applications, systems and process to meet the everchanging demands and challenges of security. The strategies that we employ include:

- Security policies
- Internet Protocol and Employee Education
- Physical and environmental security
- Operational security
- Systems development and maintenance
- Security Feature Customisation
- Policy enforced security features
- Disaster recovery and business continuity.

Security Policies

The foundation of iVvy's commitment to security is its security policies that cover physical, account, network and computer systems, application services, system services, change management, incident response and data centre security. These policies are reviewed on a regular basis to help ensure their continued effectiveness.

In addition to the requirement that all employees follow these policies, employees are educated on the important aspects of informational security, such as safe use of the Internet, working from remote locations safely and how to handle sensitive data.

Internal Protocol & Employee Education

All employees are required to conduct themselves in a manner consistent with iVvy's guidelines regarding confidentiality, business ethics, appropriate usage and professional standards.

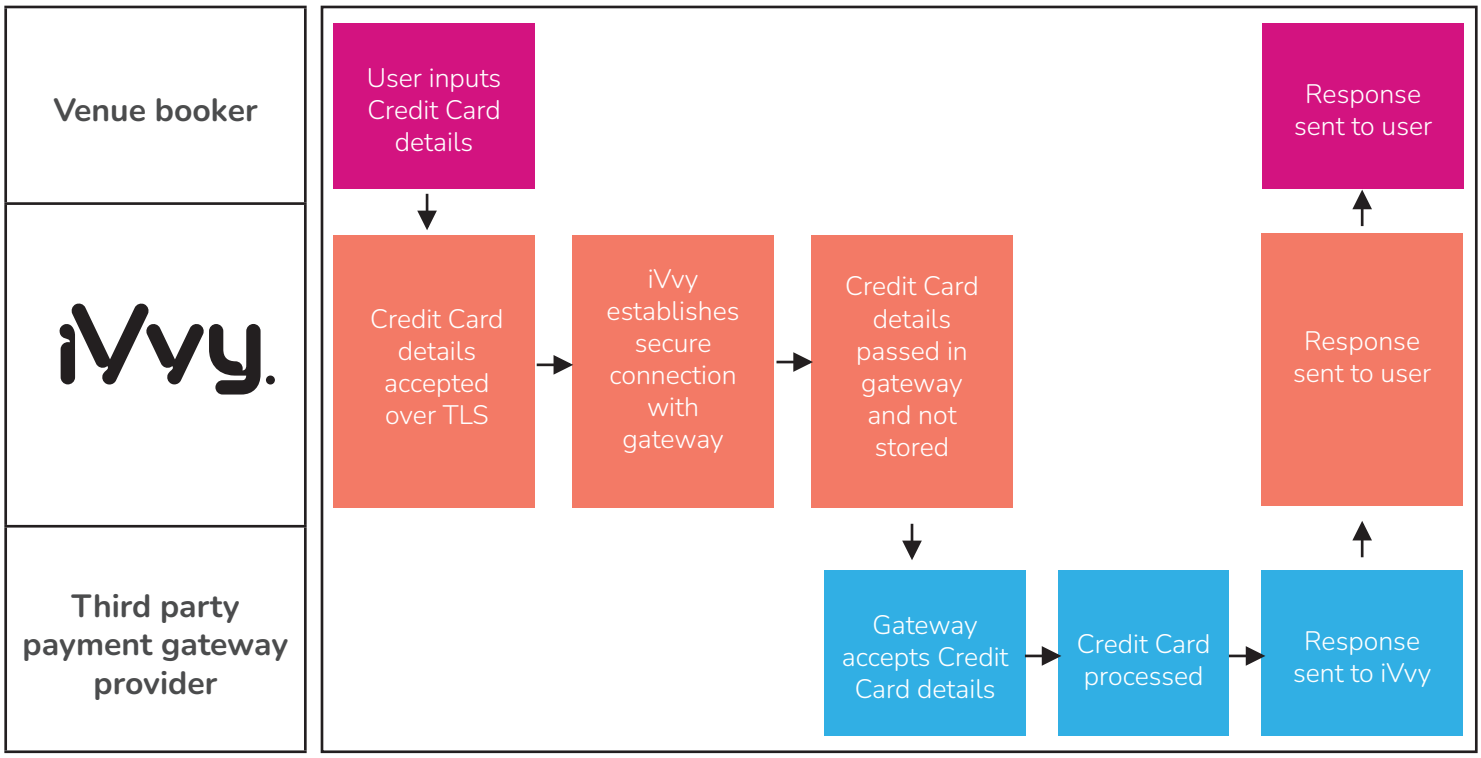
Upon hire, each employee's individual education and previous employment is checked. iVvy may conduct criminal or other security checks dependant on the role of the individual.

Employees are then required to execute a confidentiality agreement and to then read and understand the company's code of conduct. This document deals with iVvy's expectations that every employee will conduct themselves with ethics, integrity and within the law.

PCI

Ivvy has obtained PCI DSS Level 1 compliance. You can obtain a copy of the AOC by contacting privacy@ivvy.com

Credit card data is not stored within iVvy, but instead follows this flow:



ISO27001

iVvy Operates to ISO 27001 standards with an ISMS objective and scope focused on ensuring the availability, confidentiality & integrity of data within the iVvy Supplier Software, Events Software and Marketplace.

iVvy follows a risk assessment approach that includes:

1. Identify Assets
2. Identify Vulnerabilities to these Assets
3. Assess Inherent Risk
4. Identify Controls
5. Determine Residual Risk
6. Risk Treatment

iVvy's Risk Assessment, Statement of Applicability and Treatment plan is available on request for customers under an NDA.

GDPR

Under GDPR regulations, iVvy acts as a Data Processor and in addition to the security overview in this document, the platform has a range of functionality and features to make GDPR compliance easy, including:

GDPR

- **Data storage** - European customer data is stored in the UK and is never transferred by iVvy out side of this region
- **Privacy Policies** - iVvy makes it easy for you to display your Terms and Conditions, Cookie Tracking notification and Privacy Policies in platforms that your customer might engage with you on
- **Contact Anonymisation** - ivvy allows you to easily anonymise private individual information of contacts in the platform
- **Access and Communications** - You can export an XML file that will display all the information stored on a contact within the iVvy platform that can be given to an individual. iVvy also has a feature that allow individuals to see what information is stored on them with a link included at the bottom of all email campaigns sent to the individual, additionally the contact can unsubscribe from email and sms campaigns using the unsubscribe feature.

Physical & environmental security

iVvy utilises Amazon Web Services (AWS) as it's partner for hosting the ivvy application and services. AWS meets a range of compliance requirements for ensuring the physical and environmental security of your data, including:

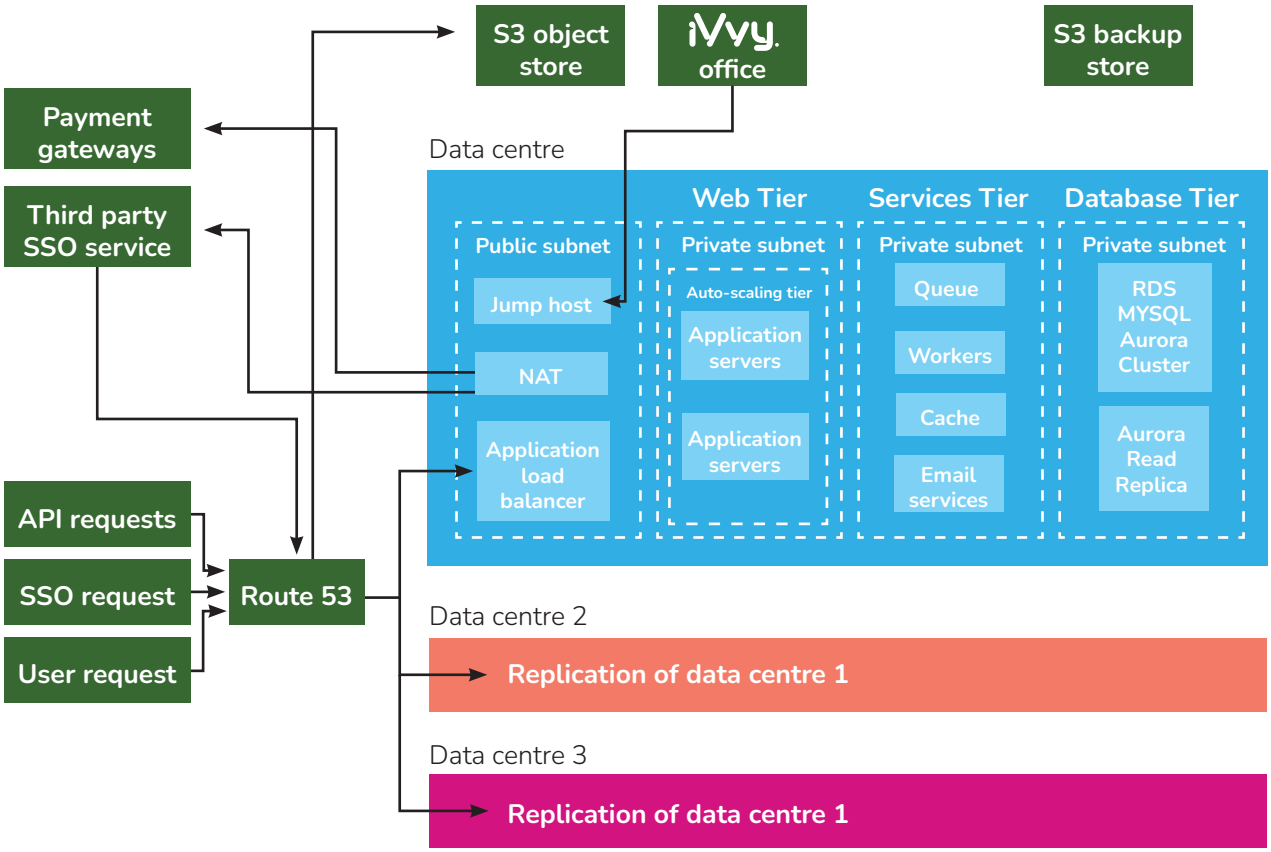
- ISO 9001, 27001, 27017, 27018,
- PCI DSS Level 1
- SOC 1, 2, & 3
- IRAP
- G-Cloud [UK], G5 [Germany]

iVvy Architecture Diagram

The following diagram outlines iVvy's architecture that is replicated in the three AWS regions iVvy currently operate in, including:

- United States
- United Kingdom
- Australia

The region you operate in, and where your data is stored is dictated by you at time of account creation on the platform. Data does not cross between regions under any circumstances unless customer initiated.



Operational Security

Network Security

iVvy uses a number of defence mechanisms to protect the network perimeter from external attacks. In order to traverse iVvy's internal and external networks, services and protocols must meet our stringent security requirements.

The components that make up the network security are as follows:

- Access to servers via shell connections is not possible except to authorised locations and personnel
- All traffic is routed and monitored through commercial grade redundant firewalls
- Network segregation is enforced using private network switches.

Operating System Security

iVvy uses proprietary software, which means that is has been fully developed by iVvy's own team of programming experts. The team uses a hardened, enterprise version of Linux specifically designed to only use the features and functionalities required of the iVvy system. This means that all others funtionalities of the system are disabled, allowing iVvy to retain complete control over the system and what it is capable of performing.

The iVvy security team are constantly researching new security measures and threats and updates are performed on a regular basis.

Data Classification and System Access

Access & Authentication

Each iVvy employee accesses the iVvy system using a two-factor authentication system comprised of a unique RFID key and a password. All passwords used comply with iVvy's strong password policy which requires a minimum password length, the inclusion of numbers and symbols, regular password resets and a Word Verification feature when multiple unsuccessful login attempts have been made.

Individuals are not aware of any of the passwords required to access iVvy's systems. At the end of a person's employment, their unique RFID key is returned to the employer and their access is fully disabled.

Authorisation Controls

Employees of differing roles are given different access rights based on their job inclusions and responsibilities. In the event that an employee requires additional access rights for a duration, a formal request for extended access permissions needs to be made by the employee, approved by iVvy Security Management and then disabled when the access right is no longer required by the employee.

iVvy employees are only granted a limited set of permissions to access client data. If the employee requires further access to client data, the client must approve this access prior to the employee accessing the client's data. Access rights to the client's data will be terminated when the employee no longer requires the client's data to perform their role.

Data Classification

Data managed by iVvy is classified according to nature of the data. This classification policy then determines the employees in iVvy that can have access to this data, and the methods required to technically secure it.

Audit Logging

iVvy logs all access to the iVvy production system and data in order to monitor any unauthorised access of the system. These logs are reviewable by iVvy security staff on an as-need basis.

Physical Security

The iVvy datacentre is one of the most sophisticated in the world and employs a range of strategies to ensure that iVvy's systems are keep at high security. These strategies include:

- Management and patrolling of the building by highly trained control staff 24 hours a day, seven days a week
- Multiple closed circuit TV points
- Secure entries and exits to the building in addition to limited access areas
- All access to the facility is logged and recorded.

Systems Development and Maintenance

Multi Layered Development

Most of the iVvy system is engineered to be run off a central set of core functionality that has been designed to avoid certain classes of vulnerabilities. For instance, the database access layers of iVvy are designed to be inherently robust against query language injection vulnerabilities, or HTML template frameworks with built-in defences against cross-site scripting vulnerabilities.

Some of the security risks solved with this approach include;

- Injection Attacks (SQL, XSS, Command, Remote Code)
- XSRF Attacks
- Session Security
- Secure File Uploads
- Creating Secure Configurations
- Password Security
- Sandboxes & Tarpits
- Security through Obscurity
- Security Implications for AJAX
- Filtering for Charsets.

Revision Control

To reduce the probability of human error or oversight in our development process, developers are required to use revision control systems to maintain current and historical versions of their source code. Once an engineer has completed code, it is submitted to a test server where the quality assurance team test the code.

Coding Reviews

iVvy's engineering team are required to partake in a peer-review process on a scheduled basis. These reviews are driven by iVvy's culture of quality engineering and integrity and are used to identify possible quality issues of individuals that may result in future security compromises.

The reviews focus on several aspects of an engineer's skills and performance including:

- Adherence to coding standards
- Adherence to style guidelines
- Quality control
- Multi-layered security testing.

Security Feature Customisation

One of the inherent challenges with security is that as you start to tighten the security of an application, you also start to remove some of its flexibility. As a result the software is written with certain features that allows a customer's domain administrator to dictate their level of security.

Password Controls

Administrators can set a range of password controls, including:

- Minimum numeric characters, password length, numeric characters and special characters
- Restricting the use of previously used passwords
- Maximum number of password changes
- Force password changes at a set number of days.

Password Strength and Length

Administrators can set password length requirements for their users. They can also visibly determine the strength of a password using a colour coded indicator when entering in their proposed password.

Login Location Restrictions

Administrators can restrict access to the system to certain IP addresses, such as the IP address associated with their office. This will help prevent login from unauthorised locations that may compromise the system security.

Maximum Login Attempts

In order to restrict the success of a brute-force-attack (where a script is designed to try all possible password combinations for a user), administrators can tell the system to lockout users for a predetermined period of time after a designated number of failed login attempts. In addition to this, users can activate Captcha (otherwise known as Word Verification) which prevents scripts from logging into a user's account. Captcha can be activated after a set number of failed login attempts have been made against a user name.

Session Timeouts

Administrators can set the system to automatically log a user out if they have not been active on the system for a set amount of time. This helps prevents the hijacking of a user account if someone has left their computer for a duration of time without logging out of the iVvy system.

Support Access

Administrators can dictate if and when iVvy support personnel can login to a user's account. A setting is also available whereby iVvy personnel must log a request for access which requires approval from the Account Administrator.

Session Identity

In order to restrict session hijacking, users can indicate the level of security that indicates that their session has not been hijacked. This can be checked against their IP address and their web browser headers.

Two-Factor Authentication

It is recommended that users in iVvy setup multi-factor Authentication to restrict access to users that both know their access credentials and also has physical access to their second authentication method. iVvy currently supports Yubico keys, and Google Authenticator.

Policy Enforced Security Features
Secure Browser Connections

iVvy users are required to use secure connections (TLS 1.2) when accessing the platform. Information is then encrypted from the moment it leaves the user's computer until it reaches iVvy.

Disaster Recovery & Business Continuity

iVvy has developed a multi-layered disaster recovery program in the event of service interruption due to a security breach, hardware failure, or natural disaster. The main principle of this system is that there be no single point of failure so that, in the event that a single server or entire data centre stops operating, there will be little to no service interruption to any individual using the iVvy system.

To this end, the iVvy software is hosted in two separate data centres, with each one acting as a failover zone for the other one. This means that data centres are physically separated and are located in lower risk flood plains. In addition to discrete uninterruptable power supply (UPS) and onsite backup generation facilities, they are each fed via different grids from independent utilities to further reduce single points of failure. Data Centres are all redundantly connected to multiple tier-1 transit providers.

Data is routinely backed-up to a minimum of two separate data-centres.

Business Continuity Objectives

iVvy's BCP plan is designed to meet the following objectives:

Maximum Tolerable Outage

iVvy's MTO goal as part of iVvy's BCP plan is 15 minutes (the maximum time an automatic failure to a secondary data centre will take).

Recovery Time Objective

iVvy's RTO goals as part of iVvy's BCP plan are:

- For Critical faults (where a large element of the Software users are unable to complete an essential business function using the Software) the RTO target is 75% of faults are restored within 4 working hours
- For High Priority Faults (where large groups of Software users are impeded in the completion of an essential business function using the Software, but a work around exists) the RTO target is 75% of faults are restored within 8 working hours.

Recovery Point Objective

For major system failure (eg: multiple data centre outages or corruption of an active database), the RPO target is 24 hours. (Based on backups occurring every 24 hours)

Backup Management

In order ensure that iVvy always has a verifiable recovery point within the last 12 hours the following requirements will need to be met:

- Data is encrypted and backed up daily basis
- The backup service is guaranteed to a minimum of 99.999% durability
- Backups are stored within a separate data centre from operating infrastructure
- Backups are verified and tested on a quarterly basis by the security and server administration teams
- Backups are encrypted with 256 AES and only ever transferred over ssl
- Backups are kept and rotated so that we maintain;
    - Every 2 hours for the last day.
    - Every day for the last week.
    - Once per week for the last 4 weeks

Service Level Agreement

iVvy operates under our standard agreement to the following SLAs:

File Type	Response Time and Type
A CRITICAL FAULT is defined as one where a large element of the Software users are unable to complete an essential business function using the Software. Standard resolution targets are 75% of faults resolved within 4 working hours. Typical examples of a critical fault are: Total Software failure, a major Software system component is inoperative or multiple Software Customer groups are impacted. **Method of Reporting:** Customer To Telephone iVvy	IVvy must acknowledge receipt of the Fault Notification within 1 hour of receipt.
A **HIGH PRIORITY FAULT** is one where large groups of Software users are impeded in the completion of an essential business function using the Software, but a work around exists. Standard resolution targets are 75% of faults resolved within 8 working hours. Typical examples of a high priority fault are: Partial loss of critical business function using the Software during normal business hours, Software system operating with severe limitations or business unit is unable to perform any function. **Method of Reporting**: Customer To Telephone iVvy	IVvy must acknowledge receipt of the Fault Notification within 3 hours of receipt.
A **MEDIUM PRIORITY FAULT** is defined as one where a small number of individuals are impeded in the completion of an essential business function using the Software. Standard resolution targets are 75% of faults resolved within 2 working days. Typical examples of a medium priority fault are: business unit able to function with reduced capacity or functionality, minimal impact system availability to the Customer. **Method of Reporting**: Log Ticket	IVvy must acknowledge receipt of the Fault Notification within 6 hours or receipt.
A **LOW PRIORITY FAULT** is defined as one where an individual is impeded in the completion of a non-essential business activity using the Software or where a temporary work around exists for an essential business function using the Software. Standard resolution targets are 75% of faults resolved within 5 working days. Typical examples of a low priority fault are: Business unit can function normally, but some individuals are affected and requests for a move, addition or change to a Customer's system. **Method of Reporting**: Log Ticket	IVvy must acknowledge receipt of the Fault Notification within 24 hours of receipt.

Conclusion

iVvy is committed to keeping information stored on its servers safe and secure and has developed a comprehensive security policy to ensure this happens. By developing policies around security, Internet Protocol and Employee Education, Physical and environmental security, Operational security, Systems development and maintenance, Security Feature Customisation and Disaster recovery and business continuity, iVvy can assure users that their privacy, confidentiality and data is extremely well protected.