SafetyCulture

August 2024

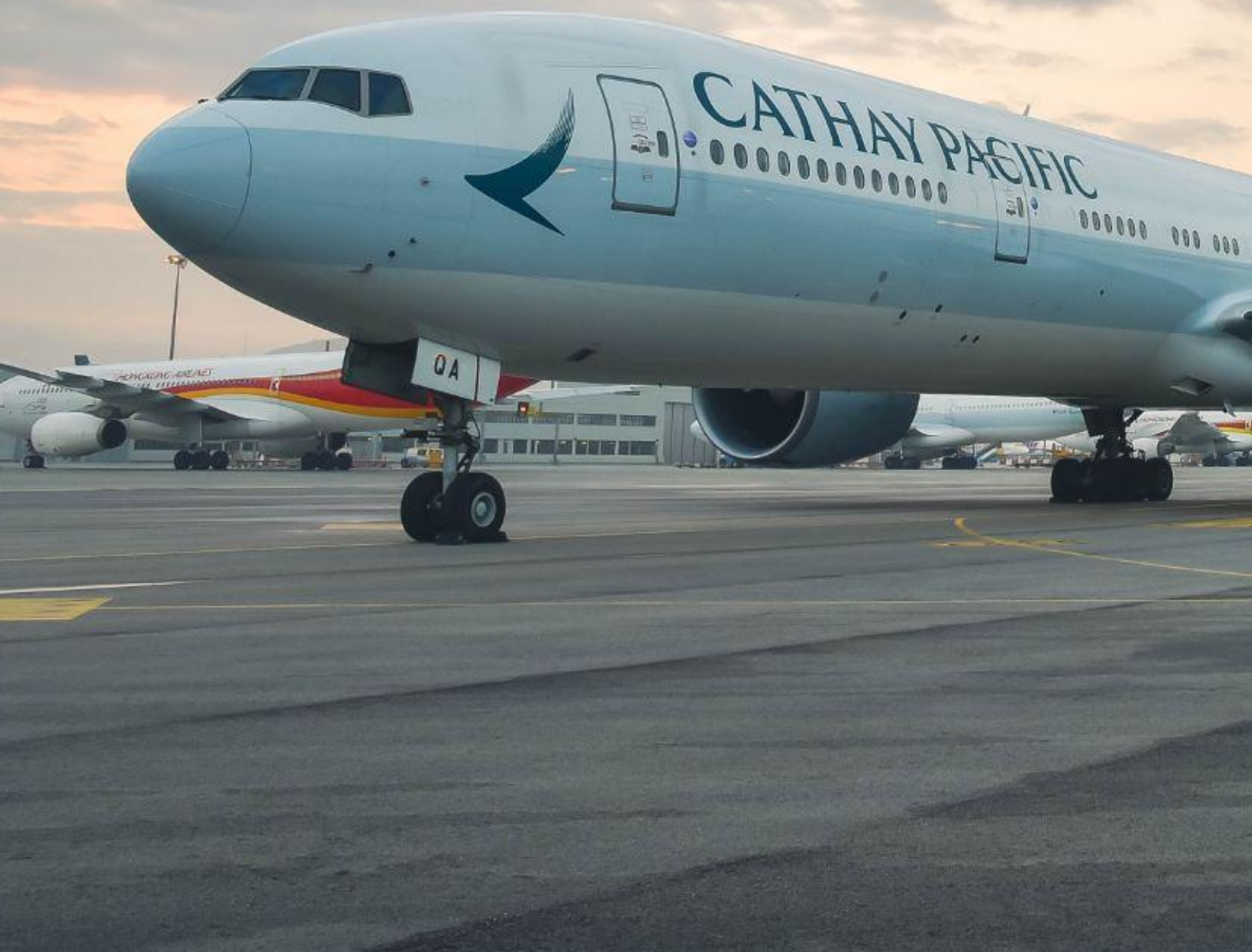
Security overview

Understand the SafetyCulture cyber security

Table of contents

Before SafetyCulture we needed someone to enter all the checklist data once they got back to the office, then run Excel analytics over it, then finally share it with the team. The Analytics gives us more comprehensive data in one area that we can share."

Deaky Wong
Line Maintenance Engineer
Cathay Pacific



Our mission

SafetyCulture's mission is to help companies achieve safer and higher quality workplaces all around the world through innovative, low-cost mobile first products.

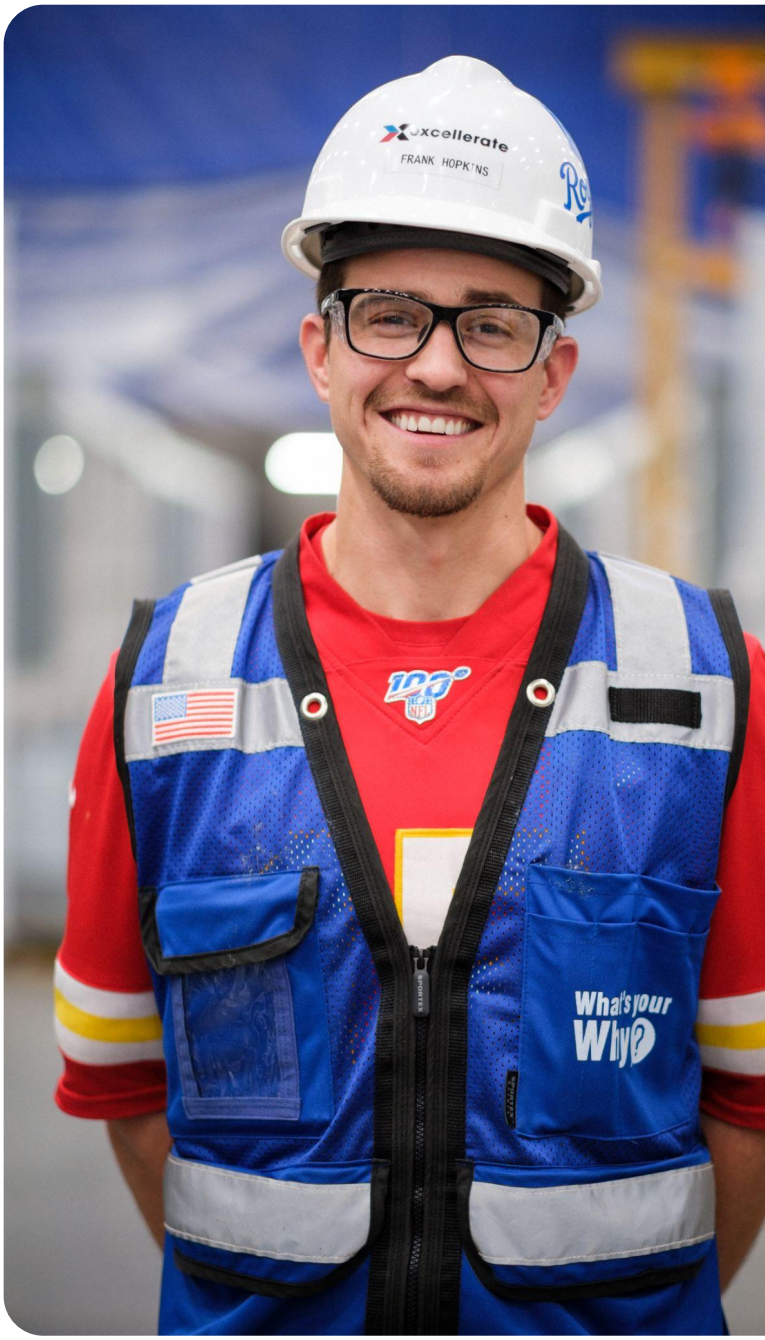
We deliver on our mission through our Software-as-Service (SaaS) products.

Our products are used by more than 75,000 companies around the world in many industries in a variety of use cases.

We take pride that SafetyCulture is seen as a world leader in products that promote safety and quality, and we know how important is in helping our customers improve their day-to-day operations.

We see our approach to cyber security as a key pillar in maintaining our status as a leader in this space, and this content summarizes how we approach cyber security as an organization.

SafetyCulture is ISO 27001:2022 certified and we follow AICPA's Trust Services Criteria affirming our dedication to customer security.



Overview

Cyber security program

SafetyCulture has an active, robust and continually improving cyber security program in place to ensure that our organization and the products we provide are secure. SafetyCulture's cyber security program employs several controls at a technical and operational level to ensure that we have an effective, defense-in-depth approach to protect from cyber attacks and secure the data handled by our Software-as-a-Services (SaaS) products.

Key features include:

- A security program aligned with industry best practice standards, including the use of cloud platforms that are compliant with trusted security benchmarks including ISO 27001 and SOC 2.
- A focus on getting the basics right, recognizing that the fundamentals of security remain the most critical. This includes:
  - ➔ Training our workforce on the importance of Security.
  - ➔ Having a dedicated security team who are responsible for keeping our organization secure from actual and impending threats to our business and the data customers entrust to us
  - ➔ Employing robust mechanisms to ensure that access to SafetyCulture's systems and customer data is carefully controlled.
  - ➔ Encrypting the customer data that we hold (both in transit and at rest).
  - ➔ Ensuring we apply patches within our IT environment and to our products as quickly as possible to minimize the opportunity for vulnerabilities to be exploited by cyber attackers.
  - ➔ Actively monitoring and testing our IT environment and our products for vulnerabilities and remedying these as a priority.
  - ➔ Having a defined process in place to provide effective support and response in the event of a security incident.

Applying due diligence to ensure our service providers are meeting industry standards when it comes to security – we know that the security of our partners directly affects us and our customers, so we choose who we work with very carefully.

The remainder of this paper provides an overview of the various parts of our security program.

Organizational security practices

Our approach to security as a company is focused on aligning with recommended best practices in recognized standards such as NIST, ISO 27001 and SOC.

Security governance

SafetyCulture has a documented set of policies, standards, and procedures that defines our approach to security as an organization. These policies and procedures are shared with all staff and reviewed and updated at least annually (and more frequently when material changes are required) to ensure our approach to security remains current
.
We focus on ensuring accountability for security throughout our company. To this end, we have an information security management forum set up with key stakeholders from across SafetyCulture that regularly meet to review and discuss security related matters, and make any decisions that have an influence on our approach to cyber security.

SafetyCulture is ISO 27001:2022 certified and we follow AICPA's Trust Services Criteria affirming our dedication to customer security.

Access controls

We ensure that access to systems in our IT environment, including the cloud platforms we use, is restricted to employees who specifically require this access for their work.

All administrator access requires multi-factor authentication, and employees accessing our environment are required to use an approved VPN solution.

Access permissions to our systems are regularly reviewed on an employee-by-employee basis and changed promptly. As part of our off-boarding process, all access to systems and services for departing employees is revoked.

Third party security

We carefully review the security practices of third parties we engage – initially and actively to ensure their practices meet industry standards and comply with our own privacy and security policies and procedures. If a third party requires access to our systems, we ensure that access is limited specifically to the purpose for which they have been engaged..

As Amazon Web Services (AWS) is one of our primary providers, we engage with them using the Shared Responsibility Model for security and compliance, ensuring there is a clear definition of who assumes responsibility for what for security. AWS is accredited by and compliant with many of the latest industry standards – more information can be found here: https://aws.amazon.com/artifact.

For the processing of financial and credit card data, SafetyCulture uses several partners (Chargify, eWay and Stripe) whose security practices comply with the Payment Card Industry Data Security Standard (PCI-DSS).

Network security

SafetyCulture's corporate networks are protected with firewalls as well as an intrusion detection system (IDS) and intrusion prevention system (IPS) technology at the perimeter provided dedicated network security devices so that we can detect and protect against any malicious traffic.

For our cloud-based platforms, we primarily use Amazon Web Services (AWS) who provide a multi-layered strategy to defend from external attacks. At an infrastructure level, AWS employs strategies such as network device access control, data segregation using firewalls and virtual private clouds to filter out malicious traffic and make use of extensive logging and monitoring to prevent network-based attacks. At an application level, we take advantage of Cloudflare's Web Application Firewall (WAF) and Distributed Denial of Service (DDoS) protection to prevent web-based and denial of service attacks against our products..

We segregate our development, test and production environments.

Logging and monitoring

SafetyCulture makes use of a centralized logging system, which includes application access audit events. These logs are retained for 90 days. We also use Amazon Elastic Load Balancing (ELB) logs to track service access requests. Logs stored in AWS cannot be modified and access is restricted to those who require it for their role requirements.

We recognize the importance of reviewing logs regularly to identify malicious user activity and identify potential vulnerabilities with our products; we have automated monitoring in place that alerts us to specific types of potentially malicious events within our global infrastructure.

Security awareness training

All SafetyCulture personnel undergo regular security awareness training for technical and non-technical roles. Additional security training material is provided to individual staff where required to ensure they are equipped to handle the specific security-oriented role challenges of their role.

Patching and vulnerability management

Patching of our IT environment is one of the most important measures we take to stay secure against a potential security breach. To achieve this:

- We use AWS System Manager to deploy patches regularly for our cloud-based infrastructure.
- We utilize mobile device management (MDM) solutions to ensure important patches are installed as quickly and efficiently.
- Our devices are secured with endpoint security technologies to detect and prevent security threats, including viruses, malware attacks and monitor for malicious activity.
- We deploy patches for the most critical vulnerabilities first, with patches being deployed to our non-production environment for initial testing before being quickly propagated across the IT environment.

Our focus

Protecting customer data

SafetyCulture takes the security of our customer's data extremely seriously. We take several steps to ensure customer data is carefully protected.

Protecting customer data

Restricting access to data

SafetyCulture takes several measures to help protect customer data from inappropriate access or use by unauthorized persons (either external or internal). Customer data is only stored in our production environment, and access to that data by SafetyCulture employees is limited only to the employees who require access to perform their standard duties. Access to customer data is managed using access control and authentication tools (including the use of two factor authentication) provided by Amazon Web Services and our other cloud partners.

Customer data is only used for purposes that are compatible with providing the contracted services, such as troubleshooting technical support requests. For full details please refer to the SafetyCulture Privacy Policy found here: https://safetyculture.com/legal/privacy-policy/

When SafetyCulture support employees need to access to specific customer data (for troubleshooting or support purposes) then SafetyCulture will always require consent from a customer before accessing this data.

We do not store or cache customer's financial data used for billing through the SafetyCulture platform and our employees do not have direct access to billing data.

Physical access to data

Customer data is hosted on infrastructure provided by Amazon Web Services which maintains the security of their sites using industry best practice controls as outlined in their security and compliance website found here: https://aws.amazon.com/architecture/security-identity-compliance/.

No customer data is stored at our physical office locations.

Data encryption

SafetyCulture has mechanisms in place to ensure that our customers' data is always protected.

At rest, all customer data stored in systems is encrypted using AES-256 with keys managed through Amazon Web Services' Key Management Service. All data is stored securely and subject to the security policies and procedures of AWS.

To protect data in transit, SafetyCulture uses Transport Layer Security (TLS) and enforces a minimum standard of TLS v1.2 using 128-bit cipher keys. We support connections with up to 256-bit cipher keys for use with an AES cipher.

Backups of data

SafetyCulture data is backed up at regular intervals to disparate encrypted data storage solutions provided by Amazon Web Services. Backups are replicated to multiple AWS facilities.
Access to data backups is restricted to only those specific employees of SafetyCulture where that access is needed as part of their role requirements. Backups are encrypted and is stored in a read-only mode.

Deletion and disposal of data

Our customer data is stored in, and subject to, the deletion and disposal procedures of Amazon Web Services. These procedures include a process to wipe secure retired media. Wiped media is then inspected to ensure to ensure the successful destruction of data.

Any SafetyCulture owned hardware that contains confidential data – including SafetyCulture backups – is subject to industry standard logical data destruction before recycling.

Securing our products

We recognize that for the bulk of customers, their principal experience with SafetyCulture will be through our products. Security forms an important part of the way our products are developed and operates.

Secure software development practices

As part of our product development process, every code and infrastructure change is stored in a source control system, versioned, reviewed, and assessed for impact prior to the release of the change into production. This review includes observance of security best practice. We also segregate our development, test and production environments, and we do not use customer data in our non-production environments.

Change control

All changes to SafetyCulture products are actively tested during their development to ensure the impact to end users is evaluated prior to deployment, and any significant changes are included in the production release notes.

SafetyCulture employs change tracking and version control systems to monitor actively and manage changes to the code base or configuration of our infrastructure. We use automated processes to deploy changes to our environments and can revert changes as required. We use Amazon CloudTrail to track any underlying configuration changes to the cloud platform on which our products operate.

Vulnerability identification and patch development

We work hard to minimize the number of vulnerabilities that arise in our products, and we recognize it is important to take proactive steps to make sure we address any vulnerabilities as quickly as possible. To that end, SafetyCulture performs annual penetration tests, and actively tests and monitors for vulnerabilities in our applications. We run a private bug bounty program because a community of independent security researchers incentivized to test our products actively to identify any potential issues will only strengthen the security of our products.

Where a vulnerability is identified (internally or externally) the issue is tracked and prioritized according to the potential severity of impact to our customers. For critical severity issues, this can include round-the-clock work by our developers until the issue is remediated.

Patches for issues are developed and released into the production environment through a continuous integration process (CI/CD) and applied as soon as possible.

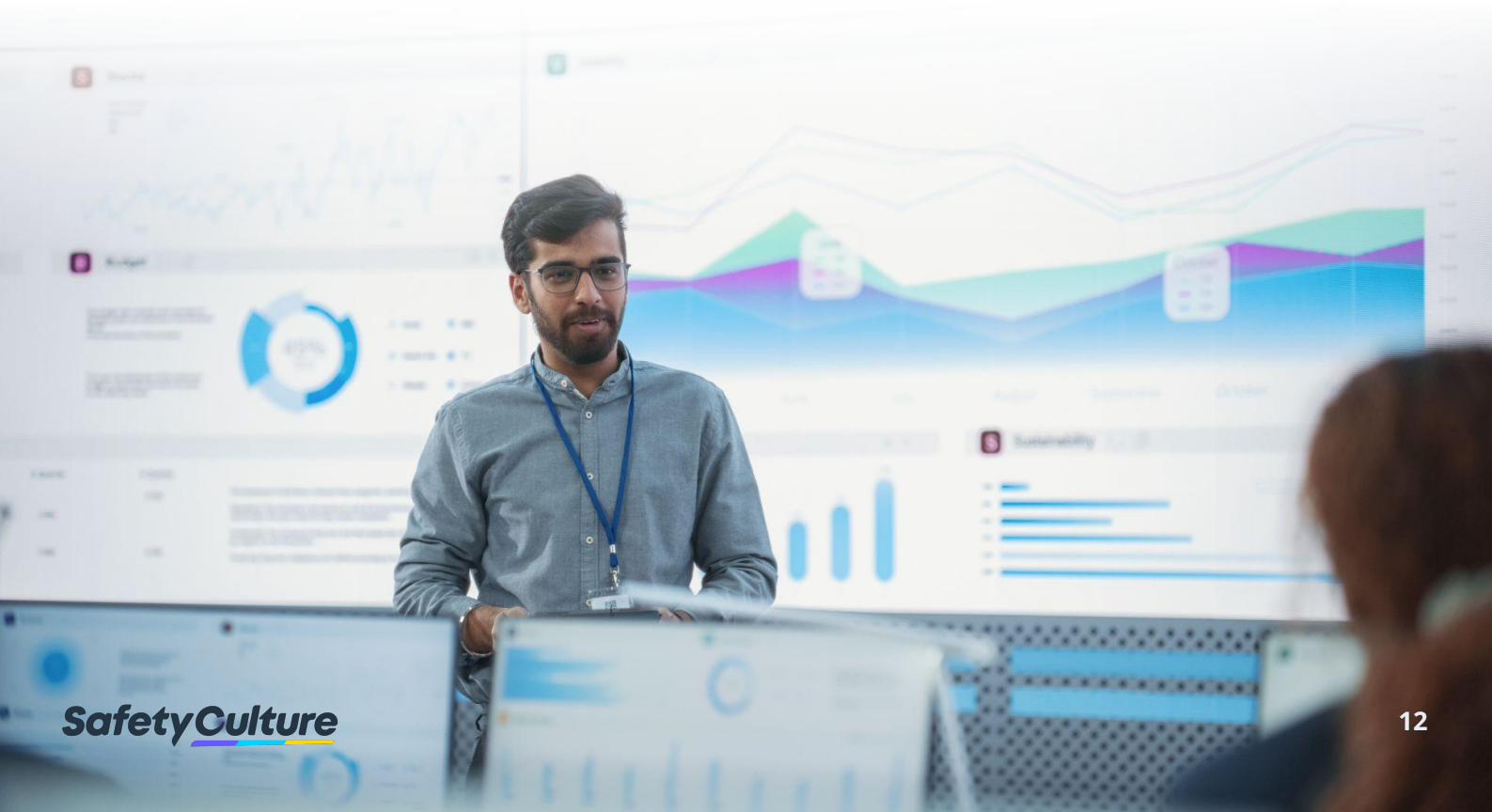
Handling security incidents

Whilst we do our utmost to prevent any security incidents, we recognize that we also need to be prepared to handle these incidents should they arise to minimize the potential impact on our customers and SafetyCulture.

We have a range of measures in place including:

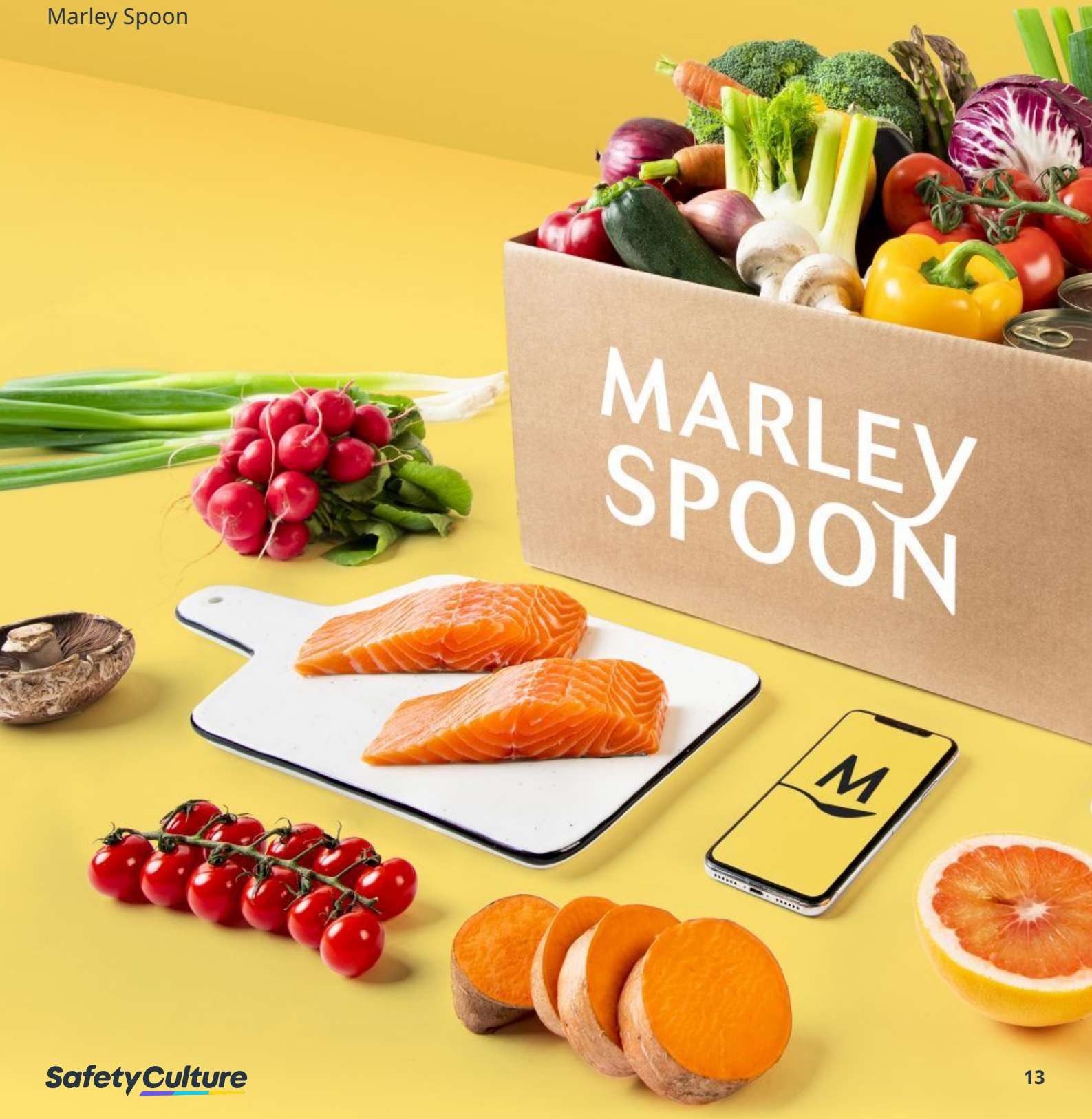
- A documented Incident Management Procedure that defines our process for handling the confidentiality, integrity and availability of our IT environment and products.
- Having a global organization to provide support during an incident.
- Established disaster recovery plans and contingency strategies which can be executed to help us maintain the continuity of operations during an incident. This includes the use of multiple geographical availability zones via Amazon Web Services and the replication of data across multiple systems in each zone. This ensures continued data access during incidents affecting system availability and provides data redundancy for the system or data storage failures.

SafetyCulture promptly alerts affected clients of major incidents impacting the availability of SafetyCulture services or data and of any incidents affecting the confidentiality and integrity their data as per our SafetyCulture Privacy Policy found here: https://safetyculture.com/legal/privacy-policy/.



“We have visibility into everything we do because of the data we capture using SafetyCulture. If there’s a threshold exception or a process that needs to be improved, all we have to do is drill down, and we’ll find it.”

Sofia Dias
Food Safety & Quality Assurance Manager
Marley Spoon



Final thoughts

SafetyCulture considers cyber security a fundamental part of our business, and of the services we provide to businesses around the world. Whilst the controls and measures we have in place extend significantly beyond what is covered here, this content serves to provide an overall understanding of the multi-faceted approach we take and our commitment to security.

If you have questions about this content or require more information about our approach to support, security or privacy please contact us at the details below.

- **Support:** support@safetyculture.com
- **Privacy:** privacy@safetyculture.com

To report security issues contact us at security@safetyculture.com

Further reading

Our security page: https://www.safetyculture.com/security

Our privacy portal: https://www.safetyculture.com/legal/privacy-portal

Our service status page: https://status.safetyculture.com/