Pickit's Approach to Security

Summary

Pickit adds impact to the work of knowledge and information workers by providing imagery to enhance their ideas, data, reports, and other messages. By integrating with the incredible Microsoft ecosystem, we can serve billions of non-professional image users and compete with visuals provided by search engines. Pickit is legalizing the volume market for photography, graphics and art and contributing to image providers along the way.

Pickit delivers a cloud-based image service inside Office. The usage of images provided as part of the Pickit library is regulated in the Terms of Use.

The development, operation and administration of the cloud-based image distribution SaaS provided by Pickit. Pickit offers a free trial for new users allowing potential customers to try the service and explore Pickit features.

The Pickit HQ is in Visby, Sweden, and the company also has a sales office in Kirkland, WA, USA. The regulatory jurisdiction is Sweden and the European Union. Pickit believes in flexibility at work, which puts great responsibility on the team when working from remote locations. This is controlled in Pickit Information Security Management (PISM).

The scope of the PISM includes all Pickit employees as well as contractors that have an individual agreement with Pickit.

Exclusions of Scope

As a cloud service, Pickit uses several 3rd party services for their operations, storage and administration. To the extent of securing their reliability and compliance with European regulations as well as having an Information Security Policy in place, these services are included in the ISMS, but not the operation of these services (Chapter 3).

The Pickit service is hosted on secure servers by Microsoft Azure in Northern Europe. The agreements put in place by Microsoft is such an example.

Pickit Information Security Management

Cross-functional teams across the Pickit organization work to secure the quality of the Pickit platform and to identify risks, developing policies to protect the data, customers and infrastructure. Two key programs at Pickit is part of the PISM:

Information Security Forum (Figure 1) – Cross-functional teams at Pickit have structured meetings to inform, asses and understand the ongoing operational quality for security and information management. It is organized to align with the ISO27001 standard. The forum has an annual management review and monthly health and compliance reviews.

Information Security Policy Program – A structured process for maintaining the Information Security Policy and for making changes when deemed necessary.

Pickit does not reinvent the wheel, so following standards and controls as well as carefully selecting providers is part of the PISM's responsibilities. Standards include:

- International Standards Organization 27001 (ISO/IEC 27001)
- Service Organization Controls (SOC2)
- Payment Card Industry - Data Security Standard (PCI - DSS)

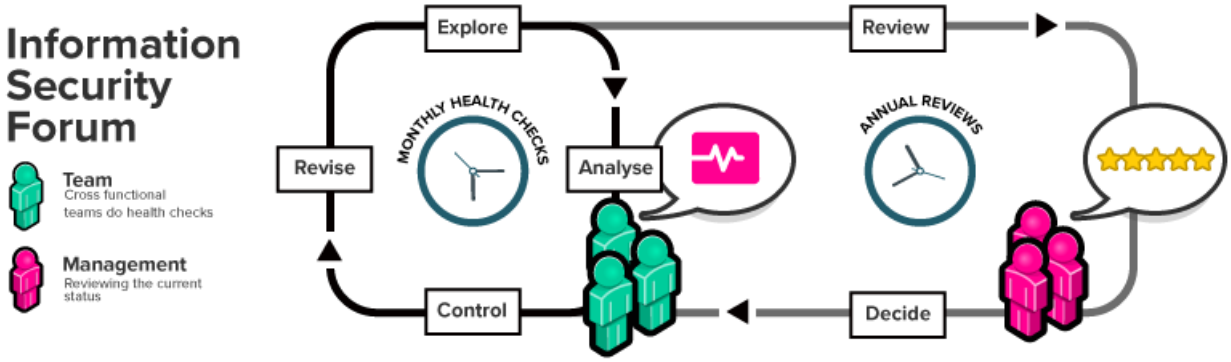


Figure 1 – Pickit Information Security Forum

I Will Panic Correctly – Incident Response Plan

The Pickit Incident Response Plan is available for all employees and outlines the process for how to act in case of an emergency or incident (e.g. data breach, hacking attempt, natural disaster, burglary etc.). This plan spells out what to expect, how to act and who to include in the pursuit to solve the situation.

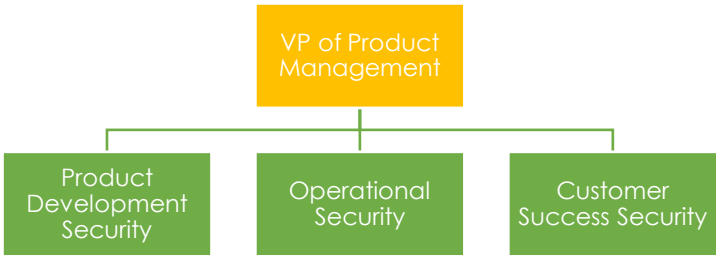
The plan will be revised and updated per changes in the office environment, system infrastructure or other changes.

Organizational Structure for Information Security

Pickit believes in privacy and security. All employees are made aware of how their work should be conducted with the customer privacy top of mind. Depending on your role, you have different access to systems and data.

Security and Risk Management has a virtual setup at Pickit, meaning that no formal roles exist. A dedicated set of Pickit employees from all departments of the organization are responsible for maintaining and enforcing the security efforts.

- VP of Product Management – Responsible for overseeing all security practices, policies and guidelines, including legislation and regulatory compliance.
- Product Development team – Platform and Service Security
- Customer Success team – Privacy and Customer Security



By combining the programs with the cross-functional organizational responsibilities, Pickit believes that it creates structure and improvement through caring and continuous revisions of policies.

- Product Development Security
  - Establish secure development practices and standards
  - Ensure project-level security risk assessments
  - Provide design review and code review security services for detection and removal of common security flaws
  - Train developers on secure coding practices
  - Coordinate penetration testing

- Operational Security
    - Build and operate security-critical infrastructure, event monitoring, and authentication services
    - Maintain a secure archive of security-relevant logs
    - Consult with operations personnel to ensure the secure configuration and maintenance of Pickit's production environment
    - Respond to alerts related to security events on Slack systems
    - Manage security incidents
    - Acquire and analyze threat intelligence
    - Manage vulnerability scanning and remediation

- Customer Success Security
    - Risk and compliance
    - Coordinate regular risk assessments
    - Manage the security awareness program
    - Respond to customer inquiries

Personnel Qualifications

Pickit's personnel practices apply to all members of the workforce (regular employees and independent contractors) who have direct access to Pickit's internal information systems and unescorted access to our office space. All staff members are required to understand and follow internal policies and standards.

Before gaining initial access to systems, all personnel must agree to our policies, NDA's and other applicable terms, pass a background screening, and attend security training. This training covers privacy and security topics, including device security, acceptable use, preventing malware, physical security, data privacy, account management, and incident reporting. Specific training is provided for employees in engineering and operations.

Upon termination of work at Pickit, all access to our systems is removed without delay.

Transfer of Knowledge

To ensure business continuation, Pickit ensures that there exists an ongoing knowledge transfer between the intangible assets. This creates a redundancy in knowledge. Within departments, this occurs as part of daily operations and between departments we have lightning talks, information sessions and regular synch-meetings to make sure that transparency and redundancy in knowledge exist. This way we strive to "back up" the knowledge held by our knowledge workers. Needless to say, Pickit document processes and information and store it in the company wiki and on secure cloud storage services.

Training is also conducted on a regular basis to ensure a high level of competency in many areas including business, information security, product and much more.

It is important to note that all information is being filtered and monitored for access to those who need it.

Privacy Policy

Pickit provides a clear, comprehensive and easily accessible privacy policy.

It can be viewed online at http://www.pickit.com/en/privacy-policy. For questions about the policy please contact support@pickit.com

Information Security Policy

Pickit perform regular maintenance and updates to their policies in to ensure that they are up to date with regulatory or infrastructure updates. Changes in the policies are communicated without delay to all company employees.

All employees at Pickit signs a document stating that they have received and are aware of the company's security policy. Pickit ensures that each employee also understand the policy. If policies are updated the employee must re-acknowledge the policies.

All employees at Pickit also sign a confidentiality agreement when they start at the company. Additional confidentiality agreements may be signed in relations to partners.

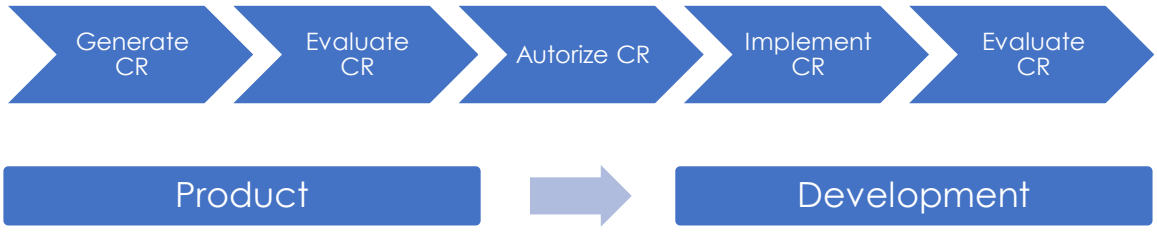
Change Management

Change is inevitable. Pickit takes pride in being agile and lean. Deliver fast and deliver often is a core part of the culture. Being customer centric mean that products need to change to fit the behaviors and needs of the customers. Change Management is done within product teams where they observe customer behavior.

As a change of current functionality is needed it is prioritized. Depending on the nature of the change it can either be moved into UX Design or directly towards Specification for technical implementation.

Change Requests (CR) are generated, specified and evaluated within product teams.

At bi-weekly stakeholder meetings, the CR's are authorized and planned for implementation.



CR's are logged in the change management log as well as within product Kanban boards.

Communicate to external stakeholders

Certain changes have an impact that affects the service for customers and partners. In good time the Changes are communicated to partners in dedicated channels per the SLA's that have been agreed upon with partners.

Key Partner Escalation
Some identified key partners have certain prioritized lanes for communication regarding planned downtime or any other disruption in the service.

Disaster Recovery Plan

Murphy's Law is something we at Pickit know surrounds us.

"*Anything that can go wrong, will go wrong*". With this knowledge Pickit takes control in minimizing the risk. Disasters are to some extent beyond control and that's where the Incident Response Plan comes in to have our customers best in mind.

Part of the Incident Response Plan is how to recover from a disaster and this is a well-structured and easily understood process which will help the company recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business operations. Additional objectives include the following:

- Ensure that all employees fully understand their duties in implementing such a plan
- Ensure that all employees are trained to efficiently execute the DR
- Ensure that operational policies are adhered to within all planned activities
- Ensure that proposed contingency arrangements are cost-effective
- Consider implications
- Disaster recovery capabilities as applicable to key customers, vendors and others

Notification Procedures

In case of a data breach or system failure, Pickit have clear policies and procedures for notifying our customers as appropriate.

Business Continuation

Keeping Pickit up and running in case of disasters, unforeseen events or due to other reasons that will put a risk on business continuation is documented in the Business Impact Analysis (BIA). Luckily, having a business in Visby, Sweden gives us a lot of structural and environmental safety where Infrastructure and the political environment is stable and reliable. Natural disasters are few, if any, and crime rates are very low.

However, there are risks for Pickit in business continuation and we strive to minimize the impact in case of these events.

The main risks for business include; Loss of key personnel, lawsuits and IT failures due to malicious attacks.

In case of an office space emergency that renders the space unusable, employees have the freedom to telecommute by work at home or at remote locations suitable for the work at hand. Optimizing the company for minimizing the need for a fixed office space creates a low risk for any business disruptions in failures at physical office locations.

In case of production environment failures our DR process ensures operational continuation.

End-user support is provided through several channels; email, chat, phone. All provided by approved partners and suppliers which are separated from Pickit production environment to keep a high availability in case of any disaster.

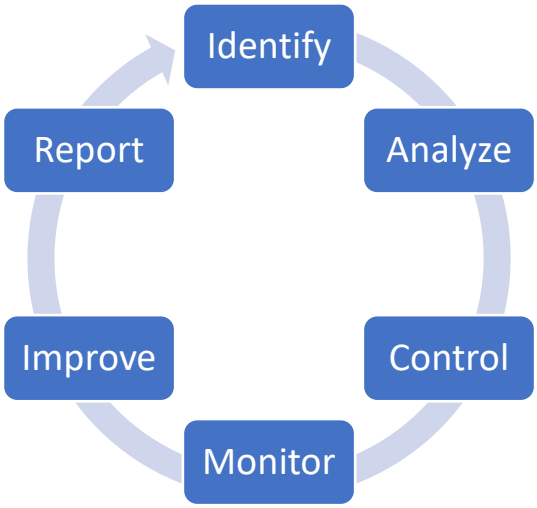
Risk Assessment

At Pickit we understand that the world goes on without us and we must be aligned with changes that happen on both macro and micro levels of operations. We work cross departmental to ensure compliance to regulatory changes not only in our IT environment but also within accounting, business and marketing.

Pickit uses external legal partners for securing compliance as well as maintaining a high level of regulatory security.

We do not seek to eliminate risk completely, but to make the best use of our resources to proactively reduce the risks posed to an acceptable level.

Our Risk Management Process



The risk management process is dynamic, with a constant feedback loop in place ensuring that we learn and adapt our approach to improve our management of risks, delivering better outcomes.

Supplier security policy

The Supplier must have an Information Security policy in place which meets applicable industry standards, and which can be subject to review by Pickit under a Non-Disclosure Agreement (NDA). This policy must comply with the laws, regulations, operational procedures and systems security configurations implemented. This policy must be reviewed on a regular basis by the Supplier. Pickit baseline is to use well known SaaS suppliers as well as reviewing their security policies. Common practice for most SaaS suppliers is to provide a set of standard policies and terms and if they meet our standards, they are approved.

For any US based supplier, we require them to be part of Privacy Shield program. GDPR alignment is also part of the requirement set for any supplier within EU and a nice to have for US-based companies. ISO27001 and/or SOC certifications are considered valuable but not needed if there exist information security documentation that show similar investments in information security.

Legal and regulatory requirements

Pickit takes great responsibility to ensure that we follow laws, regulations and legislations. We use professional legal partners in all work to ensure and enforce compliance. As a member of the European Union and being Swedish, privacy and protecting the individual is extremely important and Pickit works to be proactive and ethical in managing information.

Therefore, Pickit are:

- **PCI Compliant** Pickit is not currently a PCI-certified Service Provider. We are a PCI Level 4 Merchant and have completed the Payment Card Industry Data Security Standard's SAQ-A, allowing us to use a third party to process credit card information securely.
- **Privacy policy** are defined and transparent for all end-users. Pickit's base philosophy is to only collect the personal data needed at a timely basis, meaning that we do not collect more than necessary. As of the writing of this document we are aligned to the *GDPR*.
- **Terms of Use** for all customers define the agreement between Pickit and the customer to ensure security for both Pickit and the customer in case of any conflicts or disputes (See terms of use)
- **Supplier assessments** are done at every selection of suppliers to be included in the Pickit service. We look at information security as well as the ethical and overall SLA's.

To make sure that all policies are kept up to date, a monthly review is done in the Information Security Forum as well as being continuously observed within each department as part of daily operations.

Asset Management

To protect and manage Pickit's assets, Pickit use secure cloud services to keep information backed up and secure in case of local hardware failure or loss of personal devices. No other services than the approved are allowed. Controlled in the employment agreement is also ownership of assets, stating that all assets produced by an employee are owned by the company. In the event of a termination of employment, contract or agreement any assets owned by the company shall be returned.

Office Security

The security of the Pickit office spaces & valuable information assets is designed to keep a dynamic but secure space to work in.

The Clean Desk Policy controls how all information assets are handled and controlled within office spaces.

A Visitor Book is kept recording in an out for all visitors and all visitors are escorted.

Application Architecture

The development process
Our development process help developers to make Pickit more secure. Using the Microsoft Security Development Lifecycle as a foundation for our DevOps Processes we continuously improve our platform with *Security By Design*.

The Architecture
Pickit's platform is multi-tiered into logical segments (front-end, mid-tier and database). This help our developers to make changes to one layer without affecting the whole system, and it also help us to build secure applications.

Coding Practices
At Pickit, we leverage industry standard programming techniques such as having a documented development and quality assurance processes as well as following guidelines, such as PEP8, to ensure that the application meets security standards. In addition to that, all platform code is peer reviewed prior to being released to QA which minimizes the number of bugs that must be sent back to the developer for fixing.

Quality Assurance
At Pickit, all service changes undergo automated and manual testing including full functional testing in a QA environment before deployment to production. Continuous testing is then performed in the production environment to ensure a fully operational and high-quality service.

External Security Audits
We contract with respected external security firms who perform regular audits of the Pickit services to verify that our security practices are sound and to monitor the Pickit services for new vulnerabilities discovered by the security research community.

Penetration testing
Pickit engages independent entities to conduct regular application-level and infrastructure-level penetration tests. Results of these tests are shared with Pickit management. Product Security reviews and prioritizes the reported findings and tracks them to resolution. Customers wishing to conduct their own penetration test of Pickit application may request to do so and should contact their account representative to obtain permission from Pickit.

Legal compliance
At Pickit we have legal and compliance professional partners with extensive expertise in data privacy and security. These professionals are consulted throughout the development process and review products and features for compliance with applicable legal and regulatory requirements.

Data Security
Data security at Pickit manages how data at rest and data in flight are secured. Pickit values the integrity of our customers and work hard to ensure the security and privacy of customer data.

User Authentication
For business customers we use authentication using SSO with Azure Active Directory (AAD). The option to authenticate as defined by Django with password hashing, permission system for controlling user access is also available.

(https://docs.djangoproject.com/en/1.10/topics/auth/)

All user passwords are stored with cryptographic hash algorithms (PBKDF2)

File Storage and Encryption

- **Data in flight** are secured using HTTPS and SSH. Payments at Pickit are secured using TLS.
- **Data at rest** that can be considered sensitive are encrypted using 256-bit AES.
    - Using Azure blob storage Pickit controls access to data at rest using Azure controls. Sensitive data have strict access control while some data, such as public image files are more open.
- **Access to user files** are only accessible for authorized people in operations.

System and Network Security

Production Systems

- **Access to production systems** is only given to authorized members of the operations team. Since Pickit is hosted on Microsoft Azure we have no physical access to servers.
- **Authentication of personnel** – only authorized Pickit employees have access to services and each employee have signed and follows an information security policy stating how to manage access to services and password management.
- **Access logs** for production systems are kept in a central log repository and can only be accessed by authorized people of the operations team
- **Patching** of production systems is scheduled every 6 months and critical patches are applied as appropriate to the risk.
- **Software development processes** at Pickit are defined by product development and follow a rigid process to ensure that systems are developed and deployed with security and quality in mind. Changes to the process follow the standard change management procedure.
- **Vulnerability scans and penetration** *testing* are made on a regular basis to ensure that Pickit services are kept secure.
- **Monitoring, logging and alerting** are done 24x7x365 by dedicated services. Critical alerts generated by these systems are sent to the response teams at Pickit that escalates this as appropriate to operations management.
- **Backups** of critical data are done on a regular basis on Secure Azure Storage.

Standard Operating Procedures (SOP) for IT Management

For all routine operations Pickit uses easy to use checklists to achieve an effective, high quality output and uniform performance. We also do this to minimize the risk of human errors.

At Pickit we also work routinely with knowledge transfer is important at Pickit. To make this as efficient as possible we have procedures on how to transfer different types on knowledge to have a continuous improvement and creative work

All new personnel, regardless of competence are on-boarded using the Pickit Knowledge Center.

IT are also on-boarded together with a peer during a 5-day period where they are familiarized with the environment and are tested in the end of that period.

Data Center Security
As a SaaS, Pickit do not operate their own data centers but relies on carefully selected cloud service providers. Using Microsoft Azure, Pickit get the world at our feet. With the possibility of easy scaling, high operational stability and world class security, and we would not ask of anything less for our customers.

Infrastructure and Datacenters - Pickit is using Microsoft Azure as a cloud service provider for many reasons. Microsoft work hard making sure that their platforms are safe and secure. Pickit operates on Azure datacenters in northern Europe.

"…Cloud consumers need to rely on and trust the capabilities of cloud service providers and cloud service providers need to manage information security risks in a way that creates trust with customers."

Microsoft Information Security

Conclusion

We take security seriously at Pickit, because every person and team using our service expects their data to be secure and confidential. Safeguarding this data is a critical responsibility we must have to our customers, and we work hard to maintain that trust.