

💡 skills workflow

Information Security Policy

July 2025

João Paulo Duque Vieira CPO
joaopaulo@skillsworkflow.com

Hello,

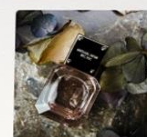
There are 5 project updates and 12 tasks planned for today.
Also 4 days until your holidays!

PROJECTS SPOTLIGHT

Most recent and delayed. Want to view all?



HP Elite New Year
Today



California Dreams
13 Jan 2019



Supreme Eyewear
05 Aug 2019



Paint & Ink
06 Jul 2019



Monika Derfflinger
11 Dec 2019



Starbucks Spring
27 Jul 2019



Sukhbirpal Dhalan
24 Jan 2019

Agenda

Optimize every corner of your agency

1 Definition & Scope

2 Responsibilities

3 Access Controls

4 Data Protection

5 Monitoring & Intrusion Detection

6 Secure Development

7 Secure Information Sharing

8 Awareness & Training

9 Reviews & Updates

10 Legal & Regulatory Compliance





1. Information Security Policy

Definition & Scope

What is at stake when handling customer data

Information Security is a critical priority

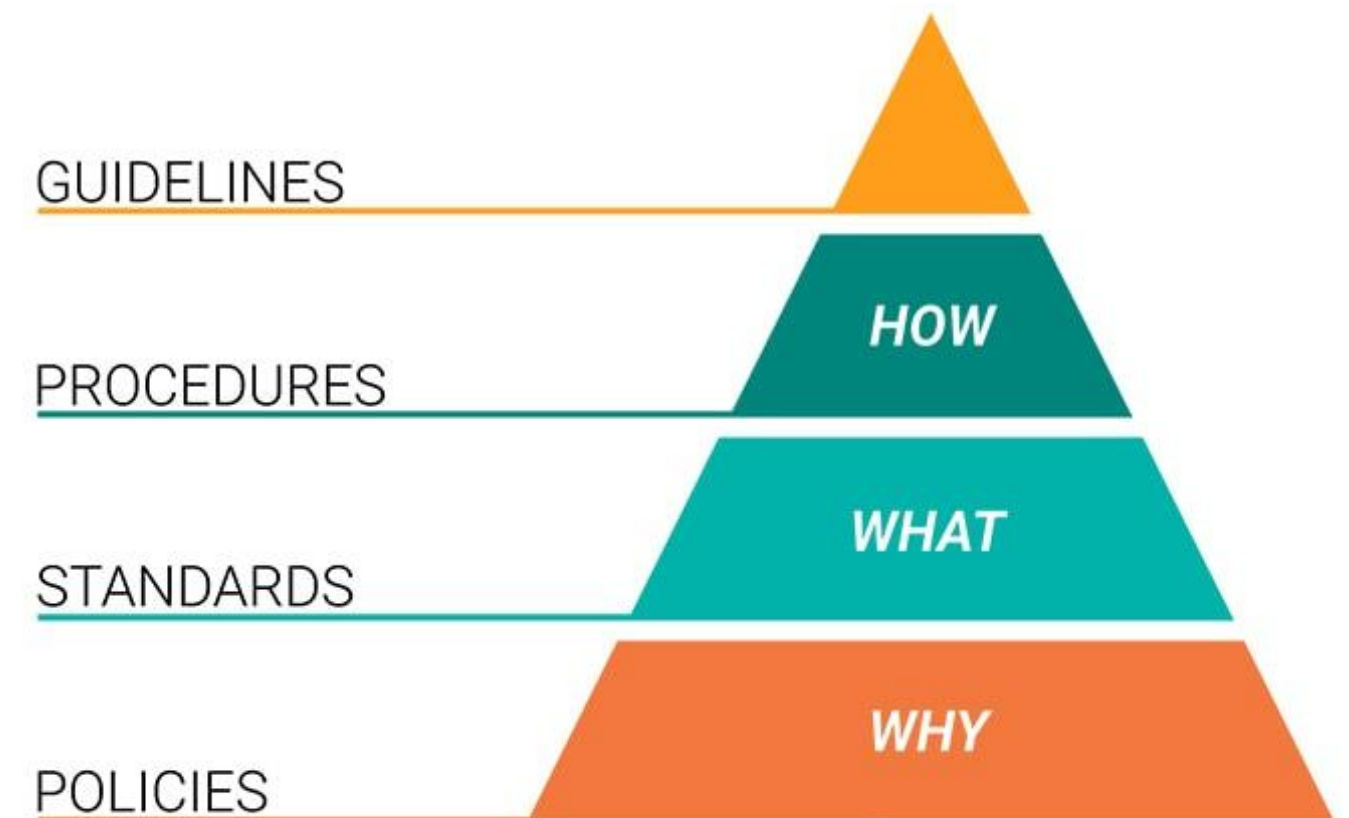
Focus on confidentiality, integrity & availability

Includes both data stored and processed

Involves everyone: employees and stakeholders

Covers the helpdesk and data from clients

In regard to: support, operation & provisioning



Responsibilities

What's the responsibility of everyone towards security



Management defines processes and sets culture
Security & IT implements and monitors controls
Support understand and follow security policies
Support reports incidents to Security & IT
Development upholds secure code practices

Access Controls

What is the attitude towards access to data and systems

Least privilege access principle to systems

MFA in every critical system and data access

Regular review of accounts to reduce access

Audit of accesses to critical systems and data

Network access restrictions to tools and data



Data Protection

Data must be always encrypted, classified and protected



Confidential data is classified and protected
Data is encrypted in transit and at rest
Backup and recovery is controlled by Microsoft
Processes are annually reviewed

Monitoring and Intrusion Detection

Continuous detection, with tools, of intrusion and threats

Continuous monitoring of suspicious activity

System logs are reviewed regularly

An incident response plan is in place

Every year pentesting is performed

Intune tools are setup to detect threats



Secure Development

Code is developed using best security practices



TOP 10

Development lifecycle is monitored with Sonar

Top 10 OWASP threats are always in mind

Vulnerability scans are performed on every build

Code review takes into consideration security

Secure Information Sharing

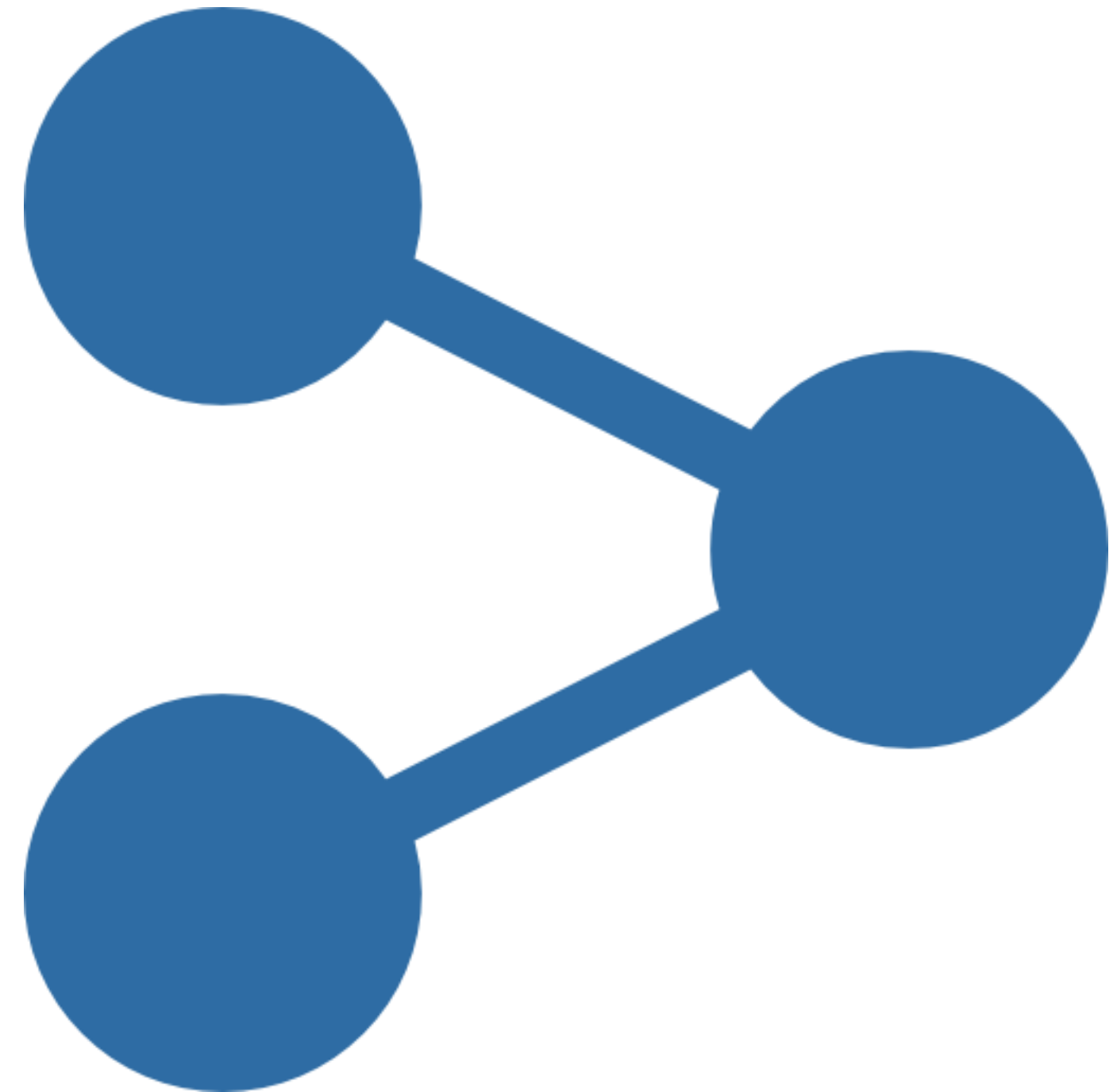
How data is shared between systems and people

Data cannot be shared outside the system

No data can be printed

Data is transferred over secure channels

Access to data checks user accesses



Awareness and Training

There's a culture of security first



All employees undergo regular training

Awareness campaigns are conducted

Users are informed of the latest threats

Deloitte audits information security processes

Reviews and Updates

How data security processes are reviewed

Deloitte reviews all processes annually

Pentesting is conduct every year

Code is reviewed on every builds

Audit logs are checked monthly

Intune is checking every data transfer always

Microsoft Azure checks their services



Legal and Regulatory Compliance

Make sure of compliance readiness for on all continents

Deloitte.

Complete compliance to GDPR rules

Compliance to SOC I and II is assured

All regulations and laws are upheld

Internal and external audits are conducted

Thank You!

João Paulo Duque Vieira CPO
joaopaulo@skillsworkflow.com



APAC • EMEA • LATAM • USA