



GRC

be connected

30
MARCH

EXPERIENCE
SHARING
EVENT



CYBER SECURITY
COALITION.be



Solvay Lifelong Learning
BRUSSELS SCHOOL. ECONOMICS. MANAGEMENT



ISACA
Belgium Chapter





Why would anyone (still) read your CyberSecurity Policy?

Marc Vael, CISM, CISSP

Thursday 30th of March 2023



@marcvael

Public



Reviewing Security Policies

Since 1995

673 security policies
reviewed/designed/implemented/maintained

(on average 24 per year)



@marcvael

Public



Survey on security policies size

1

172

Minimum

Maximum

Average?

Based on 673 security policies research between 1995-2023

@marcvael

Public



My top recommendations on effective security policy design



@marcvael

Public



1

**A boilerplate security policy
is inappropriate
because it does not reflect
how users in an organisation
actually do process digital information
amongst themselves & with others.**

definition

[def-uh-nish-uh n]

noun

1. the act of defining, or of making something definite, distinct, or clear.
2. the formal statement of the meaning or significance of a word, phrase, idiom, etc., as found in dictionaries.
3. the condition of being definite, distinct, or clearly outlined.

otics. sharpness of the image formed by an

Television. the accuracy of

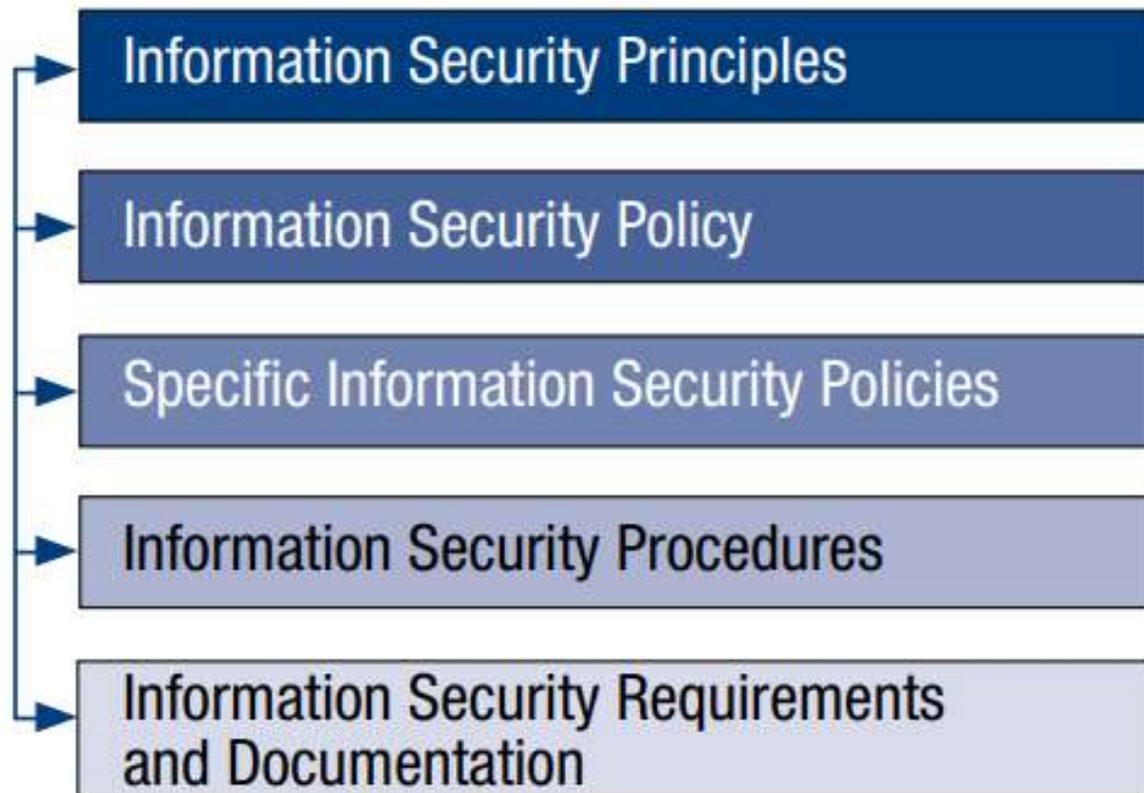
3

PROCEDURE

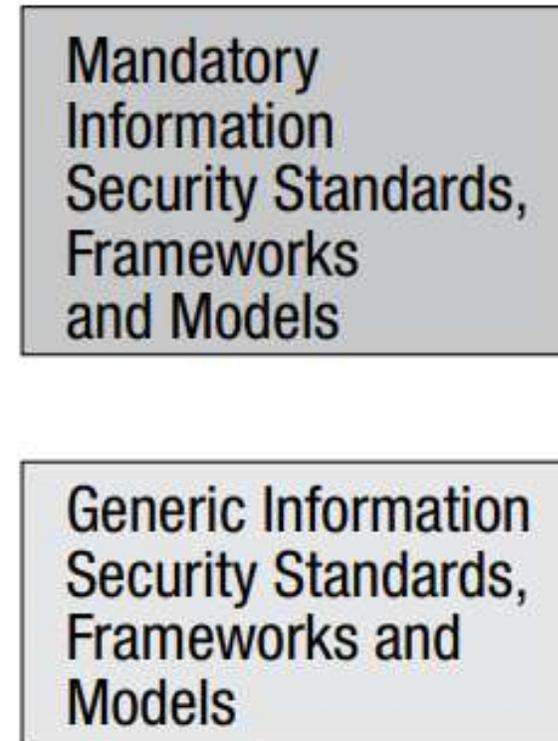
POLICIES



Policy Framework

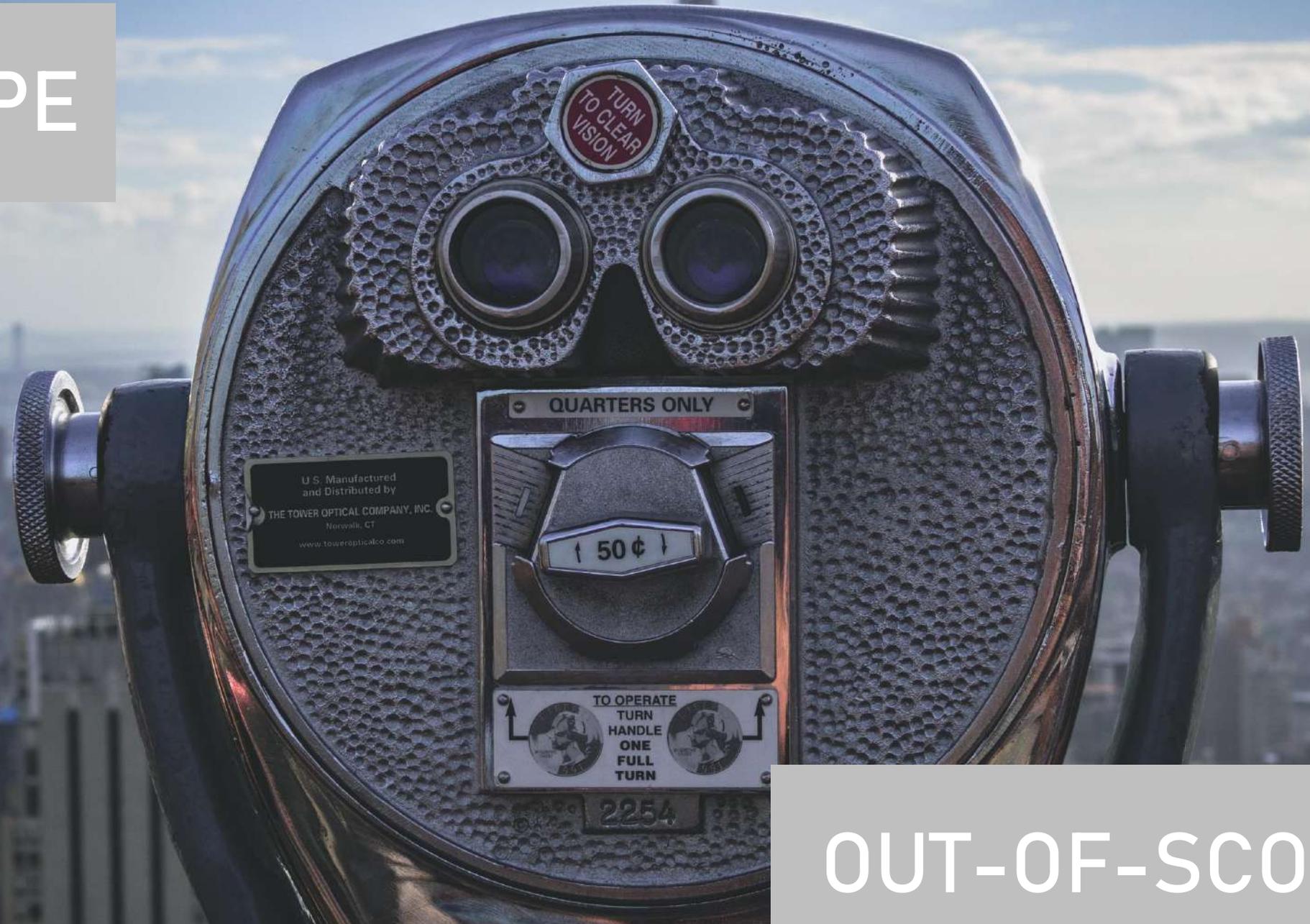


Input



4

SCOPE



OUT-OF-SCOPE

```
function(a){var b,c;bma.fine
.close-full-overlay":"close","class
"preview-preview"),render:function(){var b,depth
router.navigate(c.router.baseUrl(c.router,
this.sel.addClass("iframe-ready"),a(document.
)).removeClass("iframe-ready"),c.router,
this.trigger("preview:close"),this.undelegat
(this.sel.toggleClass("collapsed").toggleCl
"preview-device",c),this.togglePreviewDevice
"wp:wp").attr("aria-pressed",!0)},keyEvent:functio
removeClass("disabled")||(wp.updates.maybeRequest?wp
"wp:wp")))))).c.view.Themes=wp.Backbone.View.extend
"wp:wp").c.currentTheme(),this.listenTo(c.collection,
```



**MAIL
SERVERS**

DATABASE SERVERS

**WORLD WIDE WEB
SERVERS**

**PC ENGINEERING
LICENSE SERVERS**

**PC DESKTOP
COMPUTING INFRASTRUCTURE
(MICE)**

RK-20-01

RL-30-01

5

BUSINESS FOCUS



NOTICE
EMPLOYEE POLYGRAPH PROTECTION ACT

THE LAW

For Emergencies call **911** or

You Have a Right to a Safe and Healthful Workplace.
IT'S THE LAW!

1-800-321-OSHA
www.osha.gov

EMPLOYEE RIGHTS UNDER THE FAIR LABOR STANDARDS ACT

FEDERAL MINIMUM WAGE
\$5.85 - \$6.55 - \$7.25

1-866-4-USWAGE
WWW.WAGEOUR.DOL.GOV

ATTENTION EMPLOYEES

\$5.15

\$5.15

State of New York
Division of Human Rights

PERMITTED WORKING HOURS FOR MINORS UNDER 18 YEARS OF AGE

Occupational Safety & Health Notices

Employee Notice
ALL EMPLOYEES MUST READ THIS POSTER PRIOR TO EMPLOYMENT IN THIS DEPARTMENT

EMERGENCY PHONE NUMBERS CALL 911

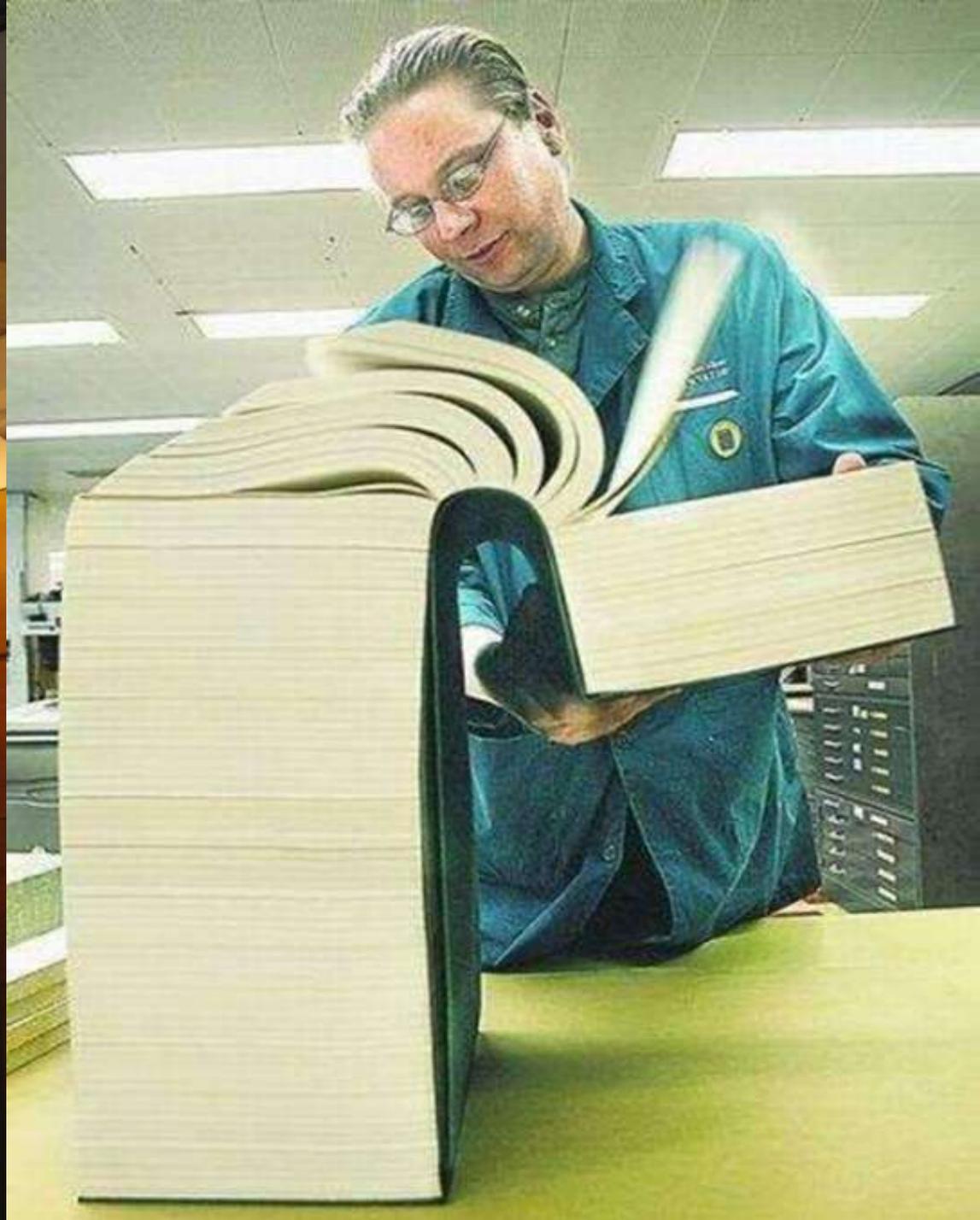
First Aid Safety Procedures

You Have a Right to a Safe and Healthful Workplace. IT'S THE LAW!

Sexual Harassment Is Forbidden By Law

YOUR RIGHTS UNDER USERRA
THE UNIFORMED SERVICES EMPLOYERS AND REEMPLOYMENT RIGHTS ACT

1-800-321-OSHA
www.osha.gov



S₁ I₁ M₃ P₃ L₁ E₁

EXECUTIVE SUPPORT



| Stakeholder | Information Type | | | | | | | | | |
|--|-------------------------------|-----------------------------|---------------------------|----------|-----------------------------------|--------------------|-------------------------------------|--|--------------------------|--------------------------------|
| | Information Security Strategy | Information Security Budget | Information Security Plan | Policies | Information Security Requirements | Awareness Material | Information Security Review Reports | Information Security Service Catalogue | Information Risk Profile | Information Security Dashboard |
| Internal: Enterprise | | | | | | | | | | |
| Board | U | | | I | | U | I | | A | |
| Chief executive officer (CEO) | U | | | A | | U | I | | U | |
| Chief financial officer (CFO) | | A | | U | | U | | | U | |
| Chief information security officer (CISO) | O | U | O | O | A | A | A | A | U | U |
| Information security steering committee (ISSC) | A | O | A | U | U | I | U | I | U | U |
| Business process owner | | | | U | O | U | | U | U | |
| Head of human resources (HR) | | | | U | | U | | | | |
| Internal: IT | | | | | | | | | | |
| Chief information officer (CIO)/IT manager | U | O | U | U | U | U | I | | U | U |
| Information security manager (ISM) | U | U | U | O | U | O | O | O | O | O |
| External | | | | | | | | | | |
| Investors | | | | | | I | | | | |
| Insurers | | | | | | I | I | | I | |
| Regulators | | I | | | | I | I | | | |
| Business Partners | | | | | | I | I | | | |
| Vendors/Suppliers | | | | | | I | | | | |
| External Auditors | | I | | | | I | I | | I | I |

A : Approver
 O : Originator
 I : Informed of info type
 U : User of info type

7

ENFORCEABLE



SECURITY EXCEPTIONS
SECURITY VARIANCES



SECURITY EXCEPTION ESSENTIALS

- Requestor
- Policy Section & Clause
- Affected Assets
- Reason for Non-Compliance
- Proposed End Date
- Compensating Controls
- Remediation Plan
- Approvals (with evidence)

9

REGULARLY UPDATED



Please wait while we install a system update

COMPLIANCE



And finally...



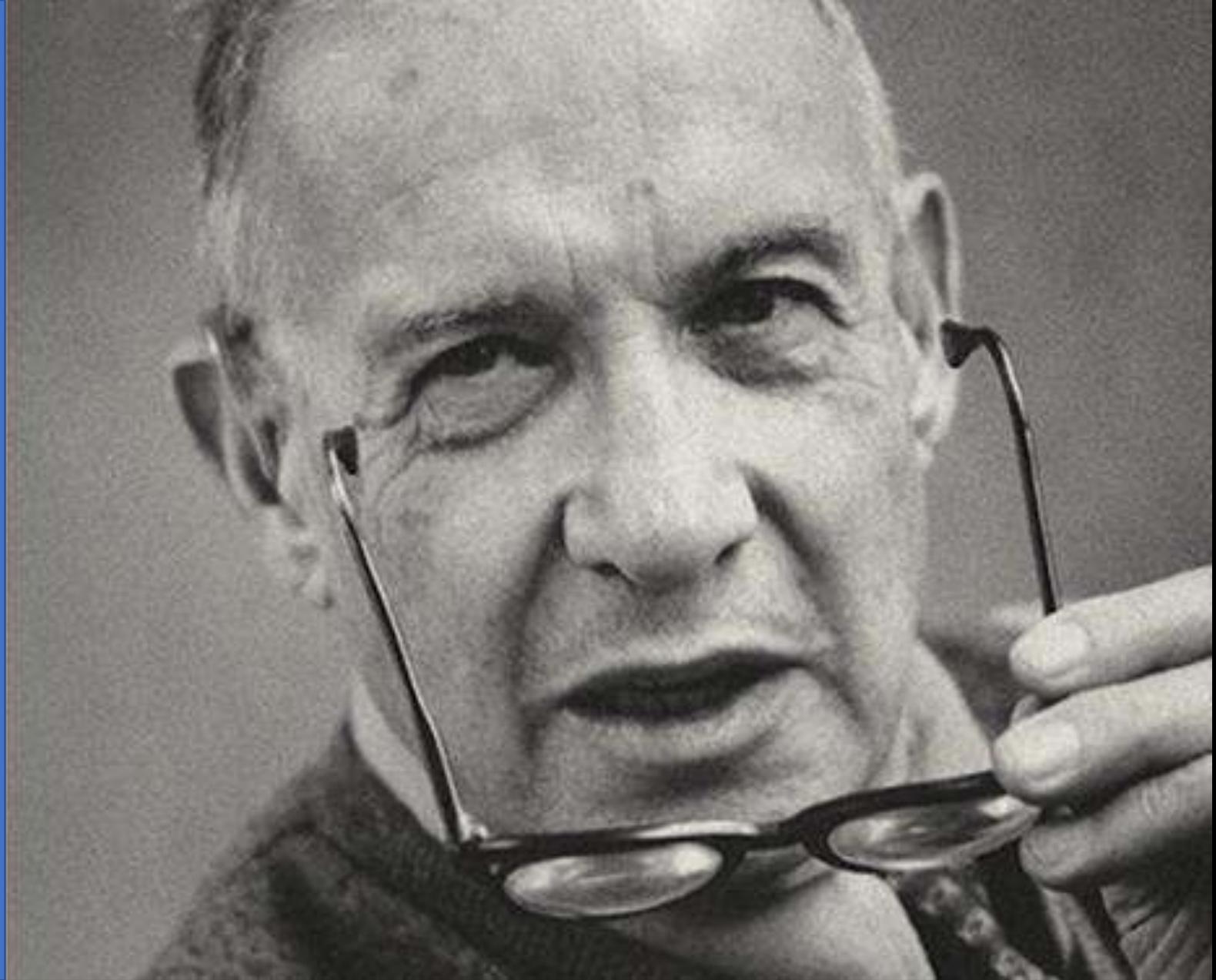
@marcvael

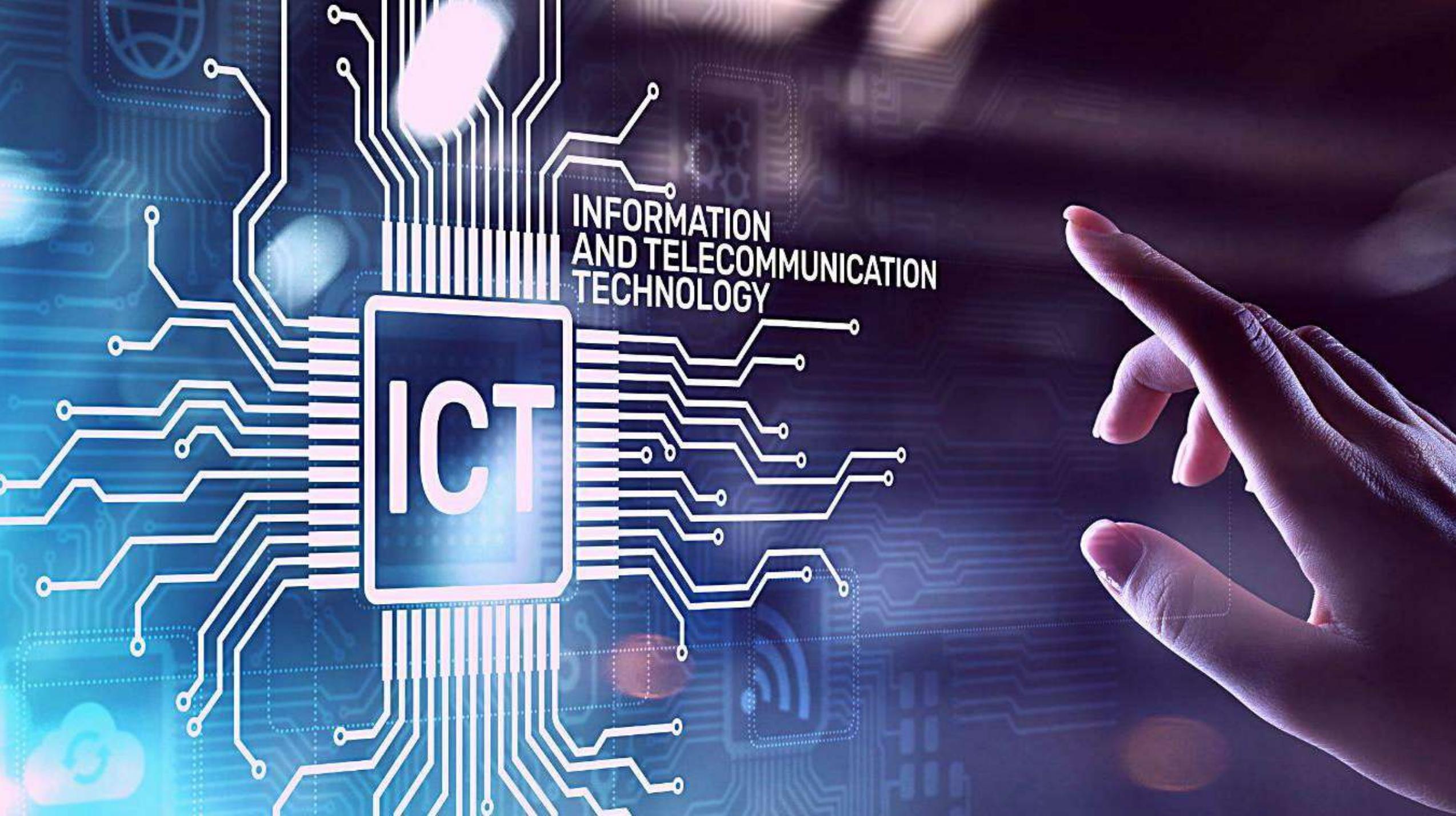
Public



CULTURE EATS SECURITY POLICY FOR BREAKFAST

Peter Drucker





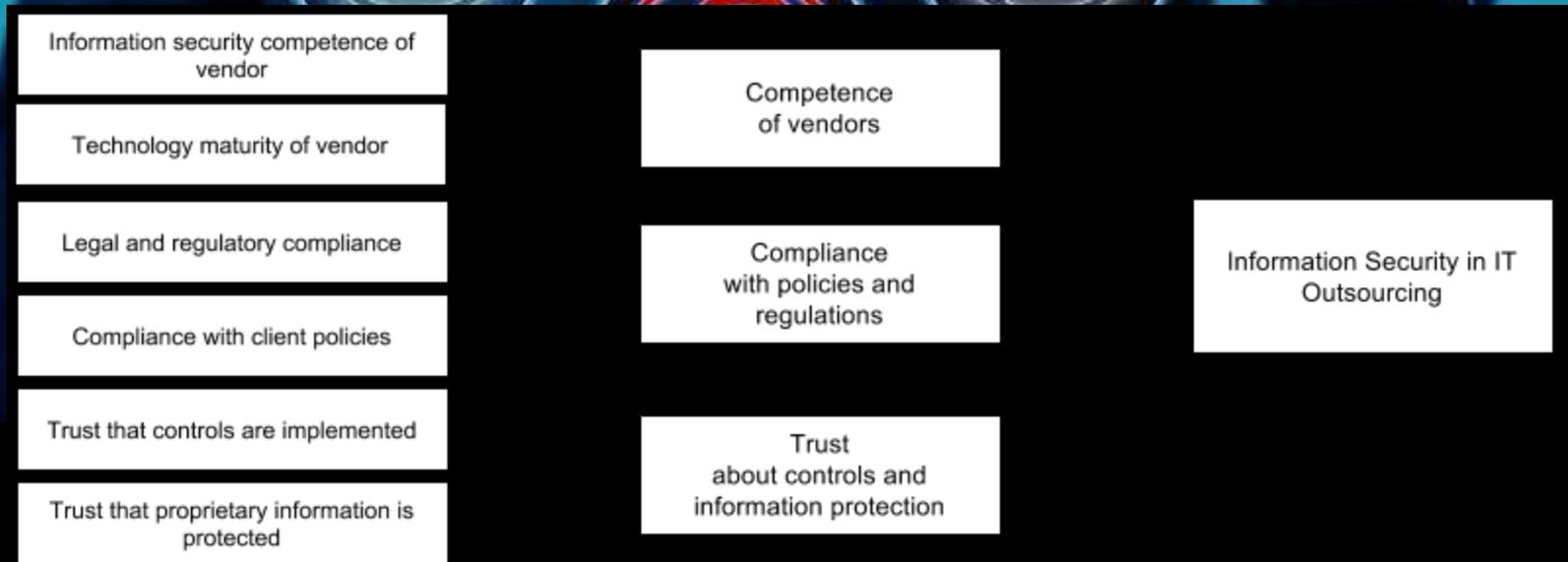
INFORMATION
AND TELECOMMUNICATION
TECHNOLOGY

ICT



Risk

MANAGED SECURITY SERVICES



A hand holding a glowing padlock icon, surrounded by digital security symbols like padlocks and data points. The background is dark blue with bokeh light effects and faint blue lines. The text 'SECURITY AWARENESS' is displayed in a white box on the right side of the image.

SECURITY AWARENESS



SECURITY PRINCIPLES

1. Support the business:

- **Focus on the business** to ensure that information security is integrated into essential business activities.
- **Deliver quality and value to stakeholders** to ensure that information security delivers value and meets business requirements.
- **Comply with relevant legal and regulatory requirements** to ensure that statutory obligations are met, stakeholder expectations are managed, and civil or criminal penalties are avoided.
- **Provide timely and accurate information on information security performance** to support business requirements and manage information risk.
- **Evaluate current and future information threats** to analyse and assess emerging information security threats so that informed, timely action to mitigate risk can be taken.
- **Promote continuous improvement in information security** to reduce costs, improve efficiency and effectiveness, and promote a culture of continuous improvement in information security.

2. Defend the business:

- **Adopt a risk-based approach** to ensure that risk is treated in a consistent and effective manner.
- **Protect classified information** to prevent disclosure to unauthorised individuals.
- **Concentrate on critical business applications** to prioritise scarce information security resources by protecting the business applications in which a security incident would have the greatest business impact.
- **Develop systems securely** to build quality, cost-effective systems on which business people can rely.

3. Promote responsible information security behaviour:

- **Act in a professional and ethical manner** to ensure that information security-related activities are performed in a reliable, responsible and effective manner.
- **Foster an information security-positive culture** to provide a positive security influence on the behaviour of end users, reduce the likelihood of security incidents occurring, and limit their potential business impact.

CORE SECURITY POLICY

| | |
|--|----|
| [REDACTED] INFORMATION SECURITY POLICY | 1 |
| TABLE OF CONTENT | 2 |
| ABOUT THIS DOCUMENT | 3 |
| 1 Introduction | 3 |
| 1.1 What is information security?..... | 3 |
| 1.2 Why is Information Security important for [REDACTED]? | 3 |
| 2 Scope | 4 |
| [REDACTED] INFORMATION SECURITY POLICY | 6 |
| [REDACTED] INFORMATION SECURITY POLICY COMPLIANCE | 8 |
| 1 Information Security Policy Variances | 8 |
| 2 Information Security Incident Reporting..... | 8 |
| 3 Information Security Policy Violations | 8 |
| 4 Information Security Questions..... | 8 |
| [REDACTED] INFORMATION SECURITY POLICY APPROVAL & AUTHORIZATION | 9 |
| ANNEX A: SPECIFIC INFORMATION SECURITY POLICIES (VERSION [REDACTED]) | 10 |
| DOCUMENT MANAGEMENT | 11 |

CORE SE

The Information Security Policy consists of the following statements:

The organization does

1. ensure all users who come in contact with protected information have completed the appropriate written **confidentiality, non-disclosure and compliance documents**.
2. **protect all IT resources** from theft, tampering, misuse, malicious software, destruction and loss.
3. ensure all IT systems are **procured and/or designed** with information security control characteristics including but not limited to:
 - o Unique user identification and authentication
 - o Data and software access authorisation
 - o System integrity protection and auditability
4. control access to confidential or sensitive information on a "**need to know**" basis.
5. control **access to information based on criteria** defined by the owner(s). The level of default protection for all proprietary information, including software, must allow no access unless specifically authorised.
6. ensure **additional authentication processes and access controls** for users entering IT systems through dial-up, internet or other communication channels.
7. provide **prompt notification to IT administrators of changes in status** (like transfers or terminations) of associates, contractors, vendors, service providers, consultants and authorized agents, or other users of IT systems that could/will affect their access privileges.
8. ensure individual and organisational accountability for the use and protection of information systems, through the assignment of **unique identification codes and authentication procedures** (like unique user id's and passphrases).
9. apply appropriate authorisation, copy protection and non-disclosure controls for all **sensitive information**, especially information released to non-group entities.
10. define and apply appropriate procedures for the use of **cryptography** (encryption/decryption) where it is deemed information may be confidential, sensitive or business critical. This must include systems that store such information with limited physical protection.
11. **prohibit the sharing and other unauthorised disclosures** of passphrases and other confidential system access controls.
12. apply additional controls to ensure the proper protection and use of Information security software features to **prevent unauthorised bypassing** of implemented information security controls.
13. produce, review, follow-up and retain **audit trails of all information security relevant logs**, data access and administration events for all systems that process protected information.
14. regularly perform **self-assessments and audits** to detect information security threats, vulnerabilities and non-compliance to the Information Security Policy.
15. define and apply all **information retention procedures** needed to satisfy internal and external requirements.
16. properly **archive, erase or dispose of information** that is no longer needed.
17. test and update **business continuity plans and disaster recovery plans** to ensure availability of resources, particularly business critical systems.

TYPICAL SECURITY SUBPOLICIES

Acceptable Use Policy

Vendor Risk Management
Policy

Secure Cloud
Management Policy

Secure Decommissioning
Policy

Network Security Policy

Security Event & Incident
Response Policy

Encryption Policy

BCM & IT DRP
Policy

Secure Authentication
Management Policy

Secure Development
Policy

Secure Data Management
Policy

Secure Compliance Policy

Secure Authorization
Management Policy

Archive & Retention Policy

Secure HR Management
Policy

Vulnerability Management
Policy

Secure Remote Access
Policy

Data Classification Policy

Secure Logging Policy

Secure Telework Policy

Authorized Software Policy
(incl security software)

Secure Change
Management Policy

Secure Patch Management
Policy

Secure Asset Management
(incl Mobile) Policy

Survey on security policies size



Based on 673 security policies research between 1995-2023

@marcvael

Public



vision action
without without
action vision
is a is a
daydream nightmare



@marcvael

Public



Contact information

Mr. Marc Vael, CISM, CISSP, CRISC, CGEIT, CISA, Guberna Certified Director

Global CISO
Danaher Packaging & Color Management Platform



 <https://www.marcvael.eu>

 marc@vael.net

 <https://www.linkedin.com/in/marcvael/>

 [@marcvael](https://twitter.com/marcvael)

President
SAI.BE
(not-for-profit IT knowledge sharing & education)



 <https://www.sai.be>

 marc.vael@sai.be

 <https://www.linkedin.com/company/sai-belgium>

 [@SAI_BELGIUM](https://twitter.com/SAI_BELGIUM)

 SAI Belgium Podcast