INFORMATION SECURITY POLICY

VERSION: 1.7

CLASSIFICATION: PUBLIC

Abstract

The overarching policy for Fourth's information security programme

Paul Cocker

FOURTH | 90 Long Acre, Covent Garden, London, WC2E 9RA, UK

Table of Contents

1. Introduction

This policy forms the keystone of our information security programme and will:

- Demonstrate the commitment of management to ensuring that Fourth is a market leader in the security and availability of information.
- Ensure our compliance with the law.
- Maintain the good name of Fourth.
- Lay out the key principles of Fourth's information security programme.
- Provide a structure for risk management within Fourth.
- Highlight policies of particular importance and provide a baseline against which policies will be developed.
- Act as a key component of our alignment with ISO 27001, an internationally recognised information security framework.
- Expand on the terms used within information security to ensure we're all speaking the same language.

Remember that information security is everybody's responsibility.

2. Scope

This policy is applicable to Fourth and its subsidiaries.

3. Purpose

- ISO 27001
    - A.5.1.1 – A.6.1.3

4. Responsibilities

Role	Responsibility
Head of Security and Compliance	• Owner • Maintaining • Communicating • Ensuring effectiveness • Implementing
Risk Steering Committee	• Approval • Review
Fourth management	• Ensuring effectiveness
Fourth employees	• Implementing

5. Management Statement

Fourth recognises the importance of our customers' information.

This is why the integrity of our systems forms a key part of our System Charter. This Charter is recognised by the Board as a keystone in ensuring the continued quality and security of our service.

Many large, publically traded companies rely on us for critical outsourcing services, and we recognise the need to adhere to an ever increasing number of standards and frameworks to demonstrate the effectiveness of our information controls.

Fourth has an information security programme to ensure the expected levels of confidentiality, integrity and availability of our customers' information are maintained.

Our Head of Security and Compliance will – in conjunction with the Board and the management team – bear the responsibility for implementing and maintaining this programme, but each employee is equally vital in ensuring its on-going effectiveness.

The foundation of our business is in providing a robust, reliable and secure platform. This programme will ensure that we continue to provide the quality of service our customers have come to expect.

Ben Hood

CEO

6. Glossary of Terms

Asset	anything that has value to the organisation
Control	something designed to mitigate a risk as part of a risk treatment
Guideline	recommended, non-mandatory controls that help support standards or serve as a reference when no applicable standard is in place
Information security event	an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant
Information security incident	a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security
ISMS	Information Security Management System, described in section 8
Policy	consists of high level statements relating to the protection of information across the business
Procedure	step-by-step instructions to assist in implementing the various policies, standards guidelines, and is used to detail processes
Process	a series of actions carried out in conjunction with one another to achieve an end goal
Residual risk	the risk remaining after a control has been applied
Risk	the consequence of the exploiting of an asset's vulnerability by a threat
Risk Steering Committee	described in section 8, this is the group responsible for managing Fourth's Risk Register
Risk owner	responsible for managing one or more risks
Risk profile	an outline of the risks to which an organisation is exposed
Risk Register	described in section 9, this is a record of all known risks to Fourth

Risk treatment	process of selection and implementation of one or more controls to mitigate a risk
Standard	specific low level mandatory controls that help enforce and support one or more policies.
Threat	anything with the potential to exploit a vulnerability e.g. a fire or a malicious hacker
Vulnerability	a weakness that could be used to endanger or cause harm to an asset through a loss of confidentiality, integrity or availability

7. Information Security

7.1. Definition of information security

Information security is the practice of defending information from unauthorised access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (electronic, physical, etc.)

The CIA triad forms a keystone of this approach.

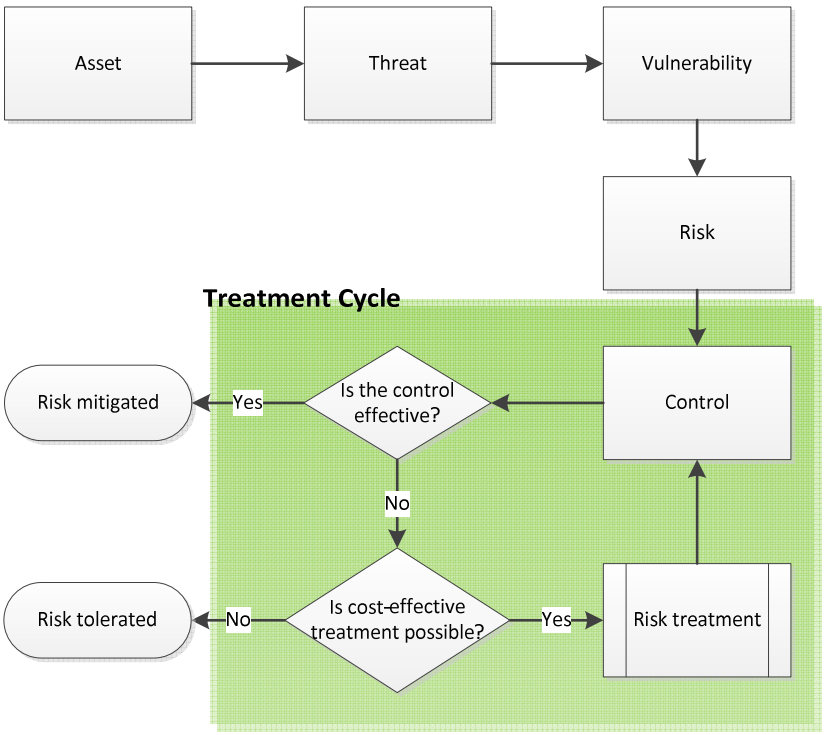
Confidentiality: the property that information is not made available or disclosed to unauthorised individuals, entities, or processes

Integrity: the property of safeguarding the accuracy and completeness of assets

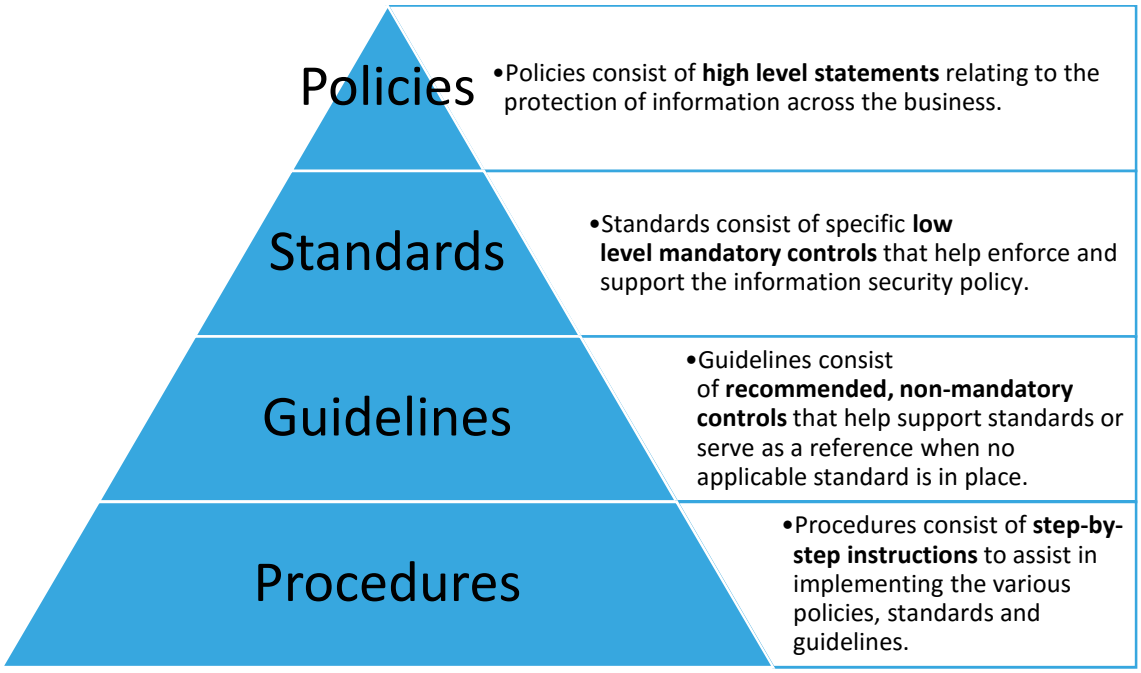
Availability: the property of being accessible and usable upon demand by an authorised entity

7.2. Definition of risk

Assets are subject to threats, which can take the form of honest mistakes, malicious hackers, or even acts of God. The way in which the threat endangers the organisation is described as a vulnerability and this creates a risk. If our controls are not effective then an appropriate risk treatment is determined and further controls may be implemented to reduce our risk profile.



7.3. Documentation framework



7.4. Information security principles

All work relating to information security will be performed according to Fourth's information security principles:

1. One vision
2. Identify the risks
3. Information matters
4. Share the knowledge
5. Always ask why
6. Doing the right thing in the right way
7. Information security is everybody's responsibility
8. Continual improvement

7.4.1 One vision

Fourth will clearly communicate its information security vision to the business. Employees will be fully aware of the business's goals and trained to meet them.

7.4.2 Identify the risks

We always examine the risk inherent in the work we carry out - including legislation we must comply with - and look for cost-effective ways to treat it. As an organisation we recognise that risk can never be truly eliminated from business, but we will always do our best to reduce it.

7.4.3 Information matters

Information is important, it has value to Fourth and it has value to our customers. We will always do our utmost to safe-guard the confidentiality, integrity and availability of information through methods which include need-to-know, least privilege and

segregation of duties. A proactive approach means that we have resolved incidents before they impact our customers.

7.4.4 Share the knowledge

We will never allow there to be single-points of failure within a team. We will ensure knowledge is always shared, be it through training or documentation.

7.4.5 Always ask why

We always ask why and we always have a good answer. We are not bound by tradition or inertia.

7.4.6 Doing the right thing in the right way

We don't go for short-term fixes; our eyes are always set on the horizon and we operate only according to facts not assumptions. We follow our agreed processes at all times. When a process doesn't work we don't just abandon it, we develop it.

7.4.7 Information security is everybody's responsibility

Information security is not a one-off thing that we complete, it is an on-going mind-set integrated into our policies, standards, procedures, and even our day-to-day decision making. We will always evaluate risk before moving forward and challenge decisions where it has not been properly considered. The responsibility for this rests with everybody and accountability is built into our systems and processes. An example is keeping your company pass with you at all times.

7.4.8 Continual improvement

We never rest on our laurels, we will continue to review and revise our approach using "Plan, Do, Check, Act" (PDCA), taking corrective action where necessary to ensure that we're operating at our best at all times.

7.5. Areas of particular importance

Fourth must ensure continued compliance with the following areas of law:

- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Employment Rights Act Part 4a 1996
- Data Protection Act 1998
- Terrorism Act 2000
- Proceeds of Crime Act 2002
- Privacy and Electronic Communications (EU Directive) Regulations 2003
- Serious Organised Crime and Police Act 2005
- Money Laundering Regulations 2007
- Bribery Act 2010
- EU-US Privacy Shield
- Criminal Finances Act 2017
- General Data Protection (EU) Regulation 2016/679

Employees will be provided with information security awareness training during induction and on a regular basis thereafter.

Employees will report any risks, information security events or information security incidents to the Head of Security and Compliance, or where they are not available, another member of the Risk Steering Committee.

All breaches of Fourth's policies by employees will be dealt with under the *Disciplinary Procedure*.

Third parties with access to, or responsible for, the processing of confidential information, are required to demonstrate that their security controls meet Fourth's standards. We have contractual agreements in place that govern the confidentiality aspects of our collaboration and have set in place controls to monitor the effectiveness of the service, including audits.

Policies, standards, guidelines and procedures will be established in alignment with Fourth's *Information Security Principle Requirements Policy* and the ISO 27001 framework.

7.6. Supporting policies, standards, procedures and guidelines

Please refer to the following items in the Employee Handbook for more information.

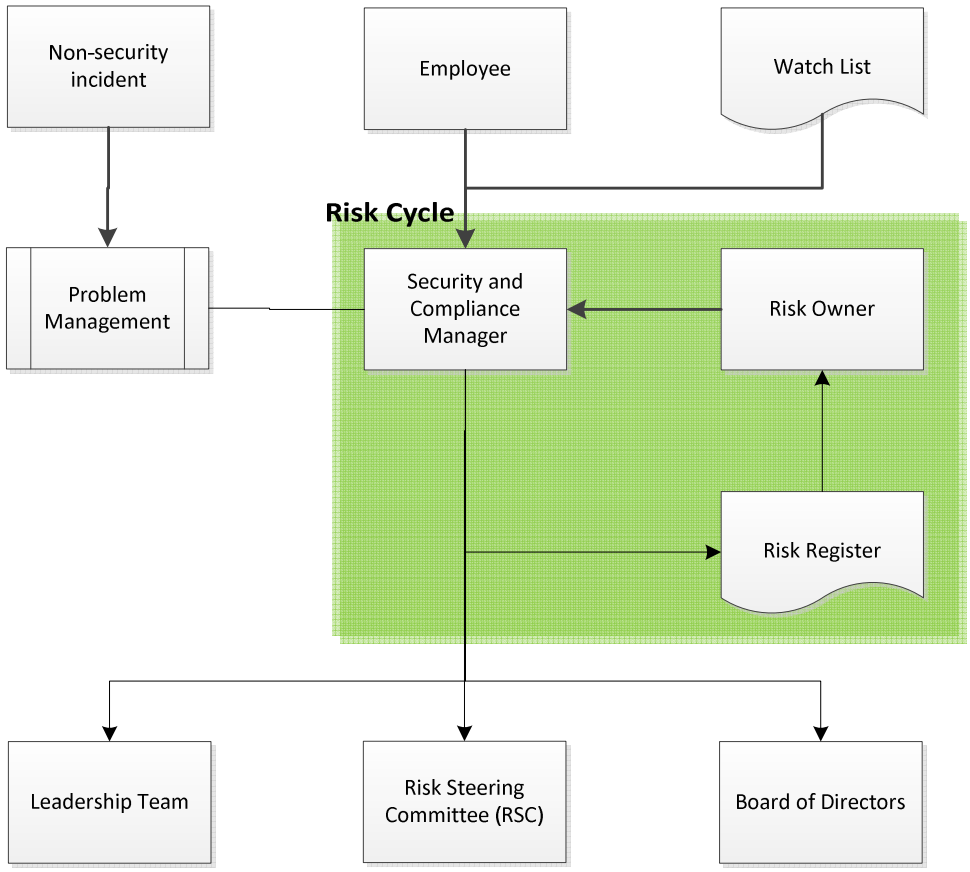
- System Charter
- Data Security Policy
- E-mail Usage Policy
- Internet Usage Policy
- Disciplinary Procedure

The proper handling of information is covered in the *Information Classification Standard*.

Requirements around passwords are in *Password and Authentication Requirements Standard*.

Further supporting policies, standards and procedures can be found on the N drive - N:\Security and Compliance\Public\Policy and Process

8. Risk Management



- **Risk Management Group**
  - Chairperson
    - Paul Cocker – *Head of Security and Compliance*
  - Participants
    - Ben Hood – *CEO*
    - Christian Berthelsen – *CTO*
    - Adrian Chalmers – *Director of Fourth Connect and Data Services*
    - Stuart Goldblatt – *CFO*
    - Mhairi Weir – *General Counsel*

8.1. Risk flow

- **Non-security incident**
  - Feeds into the Problem Management procedure
- **Problem Management**
  - Identify common root causes of incidents
  - Raise problems

    - Flag problems which represent a new risk to the Head of Security and Compliance
- **Employee**
    - Report suspected risks, information security events and information security incidents to the Head of Security and Compliance
- **Head of Security and Compliance**
    - Risks, information security events and information security incidents should be raised with the Risk Management Group
    - Maintain the Risk Register
    - Chair the Risk Steering Committee
    - Manage day-to-day running of the ISMS
- **Risk Owner**
    - Propose risk treatment
    - Implement risk treatment
    - Regular meetings with Head of Security and Compliance
- **Risk Register**
    - A record of all known risks to Fourth, their risk rating, their controls, agreed treatments and current treatment status
- **Risk Steering Committee**
    - Meets quarterly
    - Examine business risk profile
    - Review priority risks
    - Review and approve new company-wide polices, standards, procedures and guidelines
    - Discuss information security incidents
    - Agree direction of the risk management programme
    - Assign resources to meet risk profile goals

9. Risk Measurement

It is not necessary for Fourth employees to read this section unless they are part of the Risk Management Group or acting as a risk owner.

9.1. Risk scoring

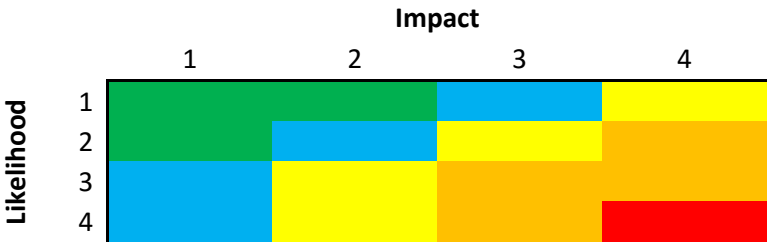
Two factors are combined to generate a risk score: the likelihood of the risk occurring and the impact to the business should it occur.

Likelihood:

1. Extremely unlikely to occur
2. Unlikely to occur
3. Likely to occur
4. Expected to occur

Impact:

1. Minimal impact
2. Moderate loss of revenue/damage to brand
3. Major loss of revenue/damage to brand
4. Major impact to the company's ability to do business



Green: Minimal risk
Blue: Low risk
Yellow: Medium risk
Orange: High risk
Red: Critical risk

See section 9.4 for how the risk score is adjusted according to control effectiveness.

9.2. Risk treatment

Once a risk has been identified and scored an agreement must be reached as to how to approach the risk. There are a number of different naming conventions, but all cover the same ground so here they will be referred to as the four Ts:

Tolerate: Retaining the risk where the cost of treatment is higher than the impact of the risk.

Treat: Making changes to reduce the probability of a vulnerability being exploited and/or putting in place a system of procedures to deal with the consequences if it is.

Transfer: Transfer the risk by making changes to contractual arrangements e.g. getting a different company to undertake the work that incurs the risk (such as insurance).

Terminate: Ceasing the activity responsible for the vulnerability thus removing the risk.

Each risk will be assigned a risk treatment. A risk which falls into the acceptable zone will automatically be assigned the tolerate treatment.

9.3. Risk register

Once a risk has been identified, scored and assigned a risk treatment it will then be presented to the Risk Management Group for approval. Once signed-off it will be entered onto the Risk Register.

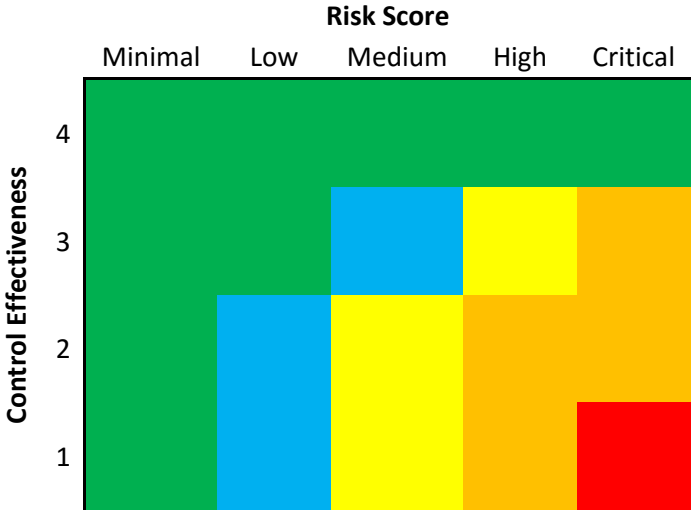
Where a disagreement over a risk occurs this will be discussed and, where possible, resolved within the Risk Management Group. If necessary it will go back to the relevant risk owner for further evaluation before being resubmitted.

9.4. Residual risk

When a control has been applied to a risk as part of a risk treatment its effectiveness must be measured to generate a residual risk score, this will allow Fourth to see whether further work is necessary to mitigate the risk to an acceptable level.

Control effectiveness is measured as follows:

1. Ineffective
2. Partially effective
3. Mostly effective
4. Completely effective



Green: **Acceptable risk**
Tolerate the risk

Blue: **Low risk**
Treatment required

Yellow: **Medium risk**
Treatment required

Orange: **High risk**
Treatment required
Include in board report

Red: **Critical risk**
Treatment required
Risk Steering Committee to be informed immediately

Document History

Version	Date of Issue	Author	Changes
0.1	01/03/13	Paul Cocker	Initial draft.
0.2	12/03/13	Paul Cocker	Added policy principles and management statement.
0.3	22/03/13	Paul Cocker	Updates to management statement, expanded definitions and content reordered and improvements to document wording.
0.4	27/03/13	Paul Cocker	Linked policy to Fourth principle requirements and added our documentation framework.
0.5	28/03/13	Paul Cocker	Minor wording changes and sign-off of management statement.
0.6	03/04/13	Paul Cocker	Added wording around third parties to 7.5 along with other minor wording changes.
1.0	16/04/13	Paul Cocker	Approved for distribution.
1.1	04/07/13	Paul Cocker	Grammatical changes and classification changed to PUBLIC.
1.2	18/07/13	Paul Cocker	Wording changes to 7.4.3, formatting change to Purpose and corrected participant list of Risk Management Group
1.3	18/07/14	Paul Cocker	Revised risk management structure and updated relevant laws
1.4	15/03/16	Paul Cocker	Defined “process” and updated the membership of the Risk Steering Committee
1.5	27/09/17	Paul Cocker	Updated risk structure, committee membership, critical risk action and relevant legislation
1.6	13/12/17	Paul Cocker	Changed risk meeting schedule
1.7	01/03/18	Paul Cocker	Add GDPR to list of legislation