PERSISTENT

Africa's Climate Venture Builder

Triple Jump

Cyber Security Toolkit

Introduction

As part of our Venture Building work we see that many companies struggle to prioritize cyber security. This was confirmed by a survey we did among SMEs in the industry. Although the number of respondents was low, the findings were clear. 70% of respondents indicate this is an important topic, only 30% have some form of training in place for their staff. Yet, research shows that this is the main reason for cyber security incidents.

As part of our work with EEGF, together with an external cyber security consultant, Triple Jump and Persistent have developed this EEGF cyber security toolkit that will allow us to more effectively work with companies to address gaps in their cybersecurity posture and minimize the risk of cybersecurity incidents in the EEGF portfolio.

The toolkit is meant for start-ups and growth-stage businesses who aim to strengthen their cybersecurity posture. The toolkit contains a number of concrete and actionable tools that can be directly shared with the company or used by the Persistent tech team to deploy together with the company. This toolkit document explains for each tool how it is to be used and what the expected outcome is.

You can download the full toolkit here!

Table of Contents

This toolkit contains a number of sections, each related to a particular objective

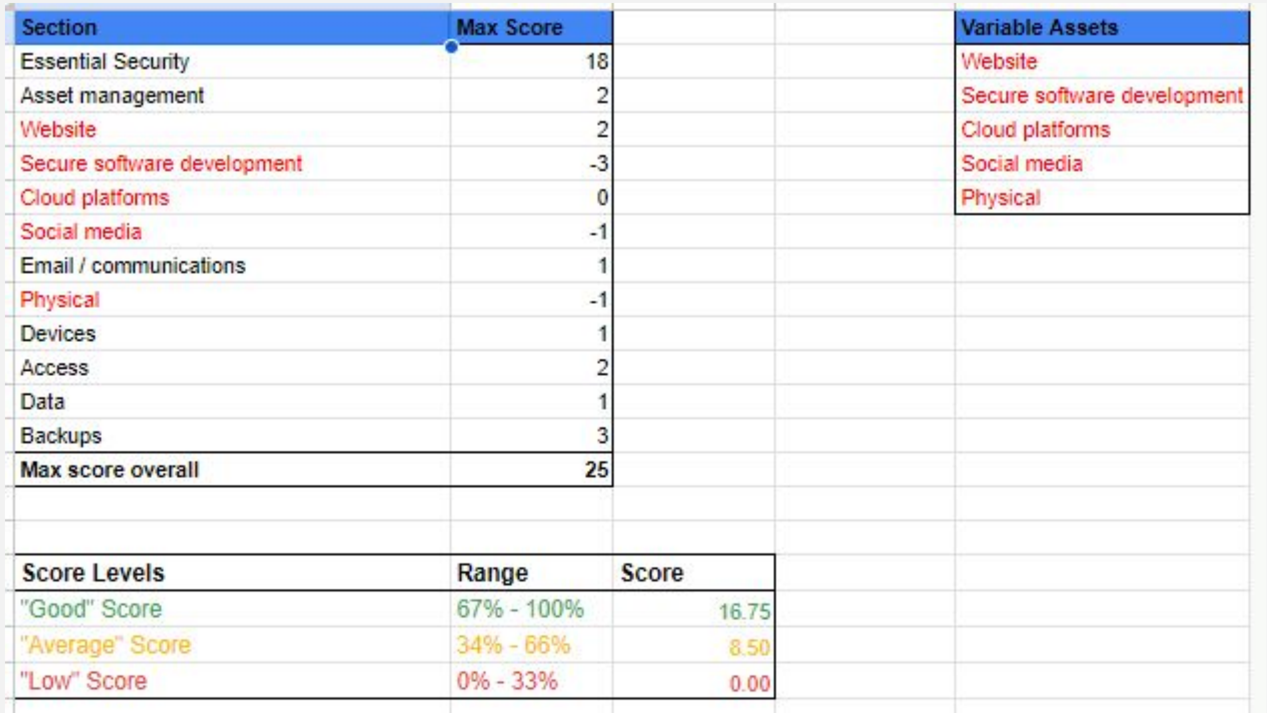
- Self Assessment
- In depth Cyber Security Review
- Staff Training
- Standard policies
  - Information Security
  - Usage Policy
  - Incident Response
  -
- Review of local regulations and support in compliance

Cybersecurity self-scan

The Cybersecurity Self-Scan (1/2)

- This survey should be filled by the company itself. We generally recommend someone in charge of IT or responsible for IT systems to start forming a picture around their cybersecurity posture.

- Each section contains a number of questions that require specific and discrete answers. Make best guesses if need be or ask for clarification in case it is unclear. Each section also has the option to provide context to the answer provided which would allow us to understand the situation better and adjust the report accordingly.



Section	Max Score
Essential Security	18
Asset management	2
Website	2
Secure software development	-3
Cloud platforms	0
Social media	-1
Email / communications	1
Physical	-1
Devices	1
Access	2
Data	1
Backups	3
Max score overall	**25**

Variable Assets
Website
Secure software development
Cloud platforms
Social media
Physical

Score Levels	Range	Score
"Good" Score	67% - 100%	16.75
"Average" Score	34% - 66%	8.50
"Low" Score	0% - 33%	0.00

The Cybersecurity Self-Scan (2/2)

- It should not take more than 10 minutes to fill, by someone who is well informed by the company's cybersecurity practices.

- Upon submission of the results, scores for each section and an overall score are automatically generated based on a underlying standard scoring mechanism.

- The tool is only as good as the answers provided. We encourage companies to be as honest and open as possible, since that will be the best starting point for any follow-up discussions.

In-depth cybersecurity scan

In-depth security scan

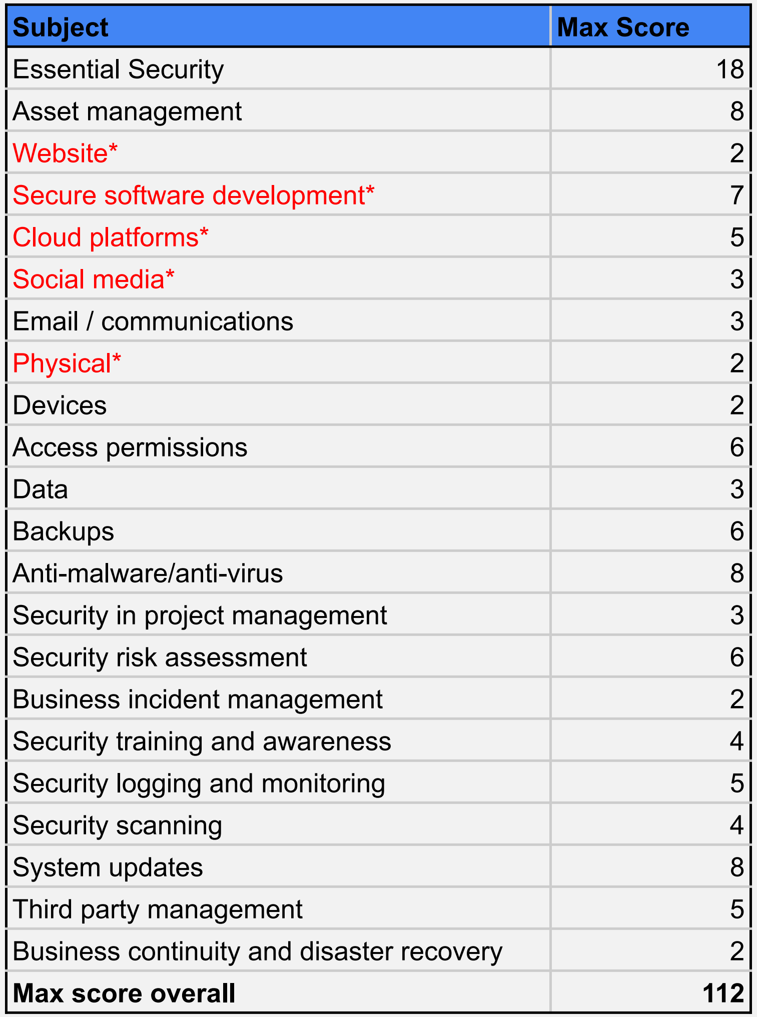
The security health check is a holistic analysis of an organisation's security level. It is an ideal starting place for a company wishing to know where they stand.

This health check should ideally be conducted on a yearly basis, in order to adapt to any emerging changes within the threat landscape.

Each section has a number of questions and points can be scored per question depending on the relevance a different weight is allocated.

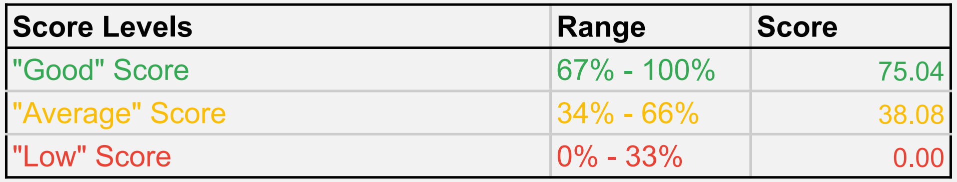
Our questionnaire has detailed descriptions and desired state and clearly indicates what evidence is required.

The output is a score per category as well as an overall score.



Subject	Max Score
Essential Security	18
Asset management	8
Website*	2
Secure software development*	7
Cloud platforms*	5
Social media*	3
Email / communications	3
Physical*	2
Devices	2
Access permissions	6
Data	3
Backups	6
Anti-malware/anti-virus	8
Security in project management	3
Security risk assessment	6
Business incident management	2
Security training and awareness	4
Security logging and monitoring	5
Security scanning	4
System updates	8
Third party management	5
Business continuity and disaster recovery	2
Max score overall	**112**

** May or may not be relevant*



Score Levels	Range	Score
"Good" Score	67% - 100%	75.04
"Average" Score	34% - 66%	38.08
"Low" Score	0% - 33%	0.00

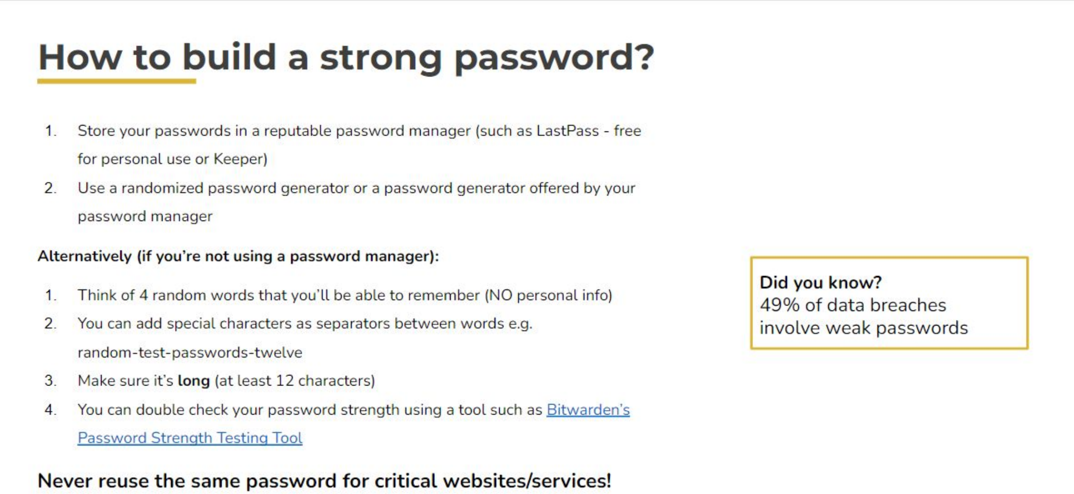
Staff Training

Staff training

An organisation is as strong as its weakest link. In cybersecurity this is often proven to the human element. People are easily compromised and this social engineering approach is where many cyber attacks have started. Whether it is an innocent looking email from what you thought was a colleague to weak passwords set by administrators. The results can be devastating.

- This is why we developed a standard staff training that can be deployed with your staff, covering the following topics like:
  - What is at stake and why is this important?
  - What is phishing and how to avoid becoming a victim?
  - How do you set a good password?
  - How to keep your devices secure and stay safe online?
  - And much more…
- We have developed a reference guide for trainers to give them a more background information about the topics presented in the training document.
- We have also included a training for trainer, so the training can be quickly deployed across the organization.
- The staff training can be done in under an hour and can be made interactive using the suggested questions.
- We recommend each new employee receives this training when starting and the training is at least repeated annually.

Staff training



How to build a strong password?

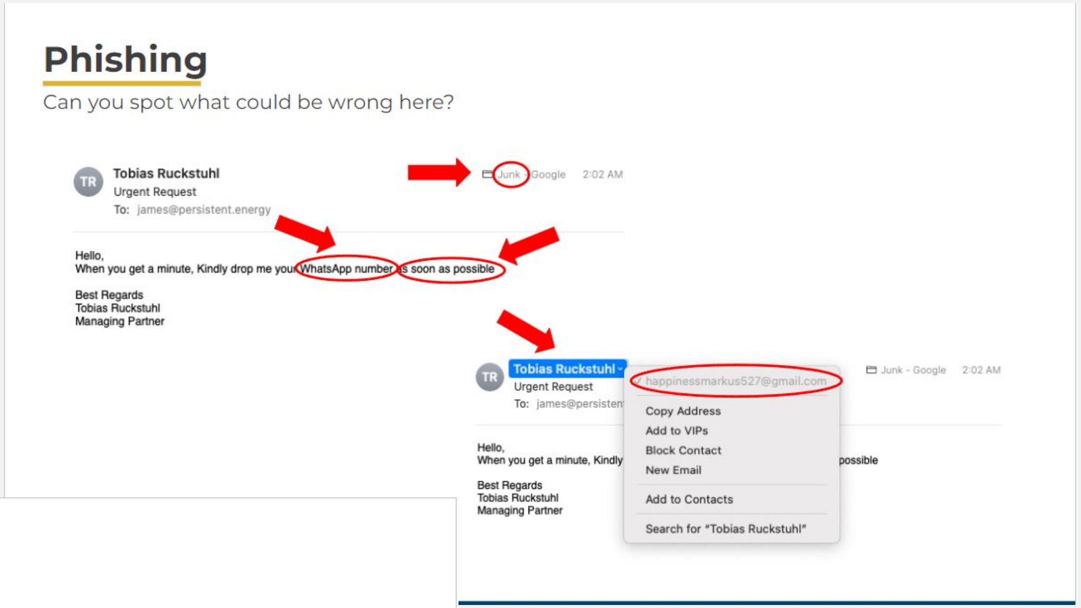
1. Store your passwords in a reputable password manager (such as LastPass - free for personal use or Keeper)
2. Use a randomized password generator or a password generator offered by your password manager

Alternatively (if you're not using a password manager):

1. Think of 4 random words that you'll be able to remember (NO personal info)
2. You can add special characters as separators between words e.g. random-test-passwords-twelve
3. Make sure it's **long** (at least 12 characters)
4. You can double check your password strength using a tool such as Bitwarden's Password Strength Testing Tool

Did you know?
49% of data breaches involve weak passwords

Never reuse the same password for critical websites/services!



Phishing

Can you spot what could be wrong here?

Tobias Ruckstuhl
Urgent Request
To: james@persistent.energy

Junk - Google 2:02 AM

Hello,
When you get a minute, Kindly drop me your WhatsApp number as soon as possible

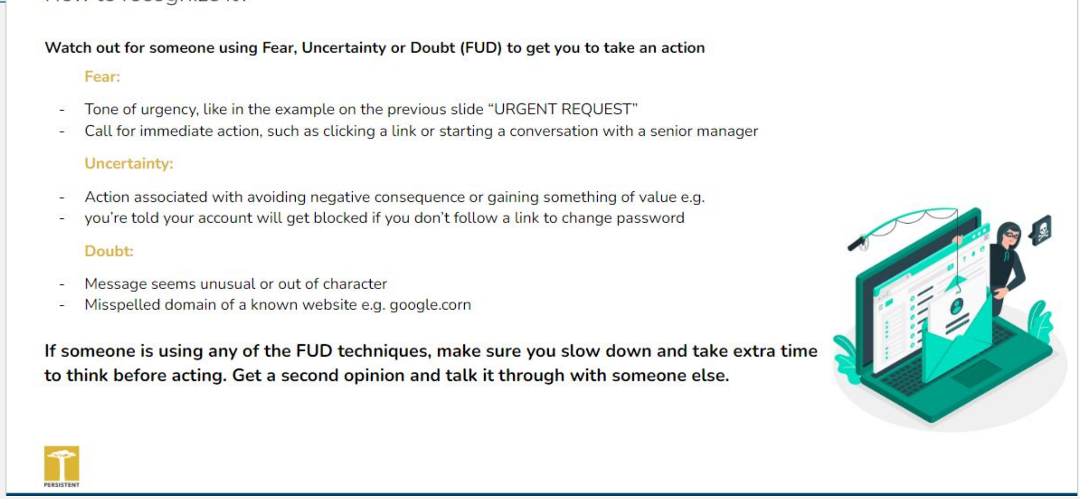
Best Regards
Tobias Ruckstuhl
Managing Partner

Tobias Ruckstuhl
Urgent Request
To: james@persisten

✓ happinessmarkus527@gmail.com

Hello,
When you get a minute, Kindly possible

Best Regards
Tobias Ruckstuhl
Managing Partner



Phishing

How to recognize it?

Watch out for someone using Fear, Uncertainty or Doubt (FUD) to get you to take an action

Fear:

- Tone of urgency, like in the example on the previous slide "URGENT REQUEST"
- Call for immediate action, such as clicking a link or starting a conversation with a senior manager

Uncertainty:

- Action associated with avoiding negative consequence or gaining something of value e.g.
- you're told your account will get blocked if you don't follow a link to change password

Doubt:

- Message seems unusual or out of character
- Misspelled domain of a known website e.g. google.corn

If someone is using any of the FUD techniques, make sure you slow down and take extra time to think before acting. Get a second opinion and talk it through with someone else.

Policies

Introduction Policies

As part of the toolkit we offer three key policy templates that can be easily adopted by companies. These policies are not intended to allow a company to check a box, but are intended as meaningful guidelines that help enforce certain common place practices and keep the company's information safe and secure.

The three policies are:

- An information security policy
- An Staff usage Policy
- An incident Response Plan

General Information Security Policy

These are general Information Security Policies that every company should have in place. See image for overview of contents.

- It does not guarantee 100% compliance with international standards such as ISO27001, as these tend to go much further than needed for the SME space.
- It is not expected a company is compliant from day 1, we rather recommend companies look at this as their ideal scenario and make a plan to work towards full compliance.

How to implement

- Each policy has unique sections that can and should be amended based on the company's specifics.
- Where needed we will use findings from the self scan and/or deep dive to propose specific changes.
- We recommend the policy is reviewed annually for needed changes as well as compliance.
- The adopting company should verify compliance and generate an overall compliance score so progress towards full adoption can be tracked. A clear internal owner should be assigned!

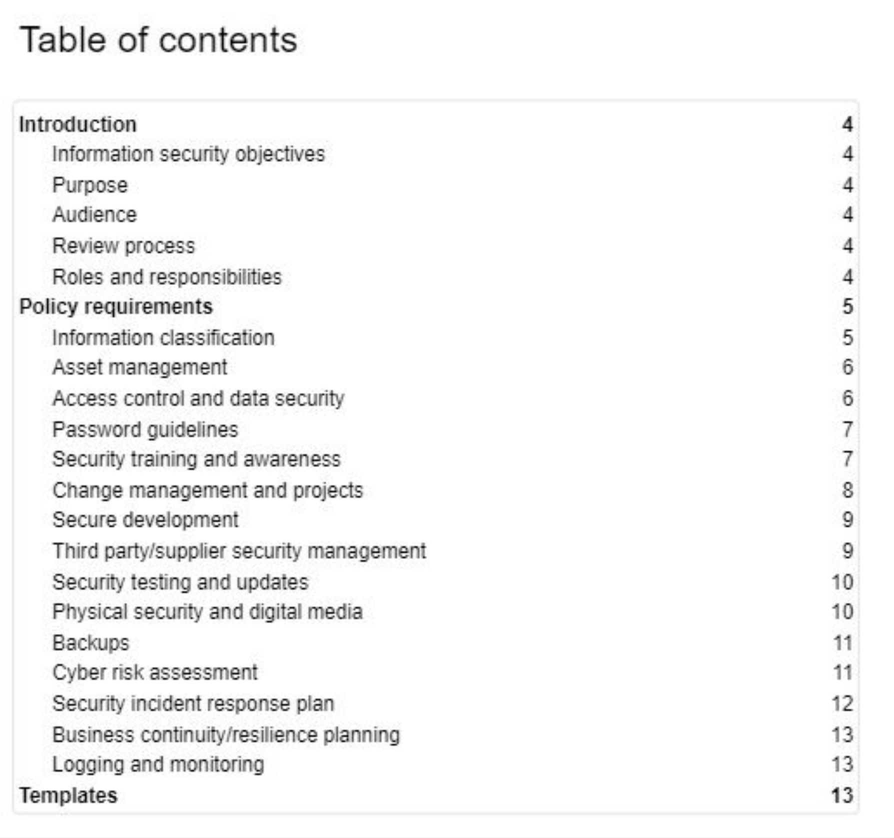


Table of contents

Acceptable Use Policy

Aside from general Information Security Policies, it is important that it is clear what is expected from staff when it comes to the use of IT resources. People tend to be the most exploited weakness in IT systems. Having a crystal clear Acceptable Use policy which is well communicated is a key policy any organisation should have in place.

An acceptable use policy defines how employees and contractors will use organisations systems, data and devices. It states what types of usage is prohibited and how to look after organisational assets to ensure employees can carry out their job roles, and organisation assets remain protected from data security breaches and other types of business risk.

<u>How to implement</u>

- Each policy has unique sections that can and should be amended based on the company's specifics.
- Where needed we will use findings from the self scan and/or deep dive to propose specific changes.
- We recommend the policy is reviewed annually to ensure it remains relevant and up tp date with the latest risks.
- The policy should be strongly embedded in HR and training processes so new staff are trained and existing staff are reminded. It is recommended that the policy is issued together with the employment contract.

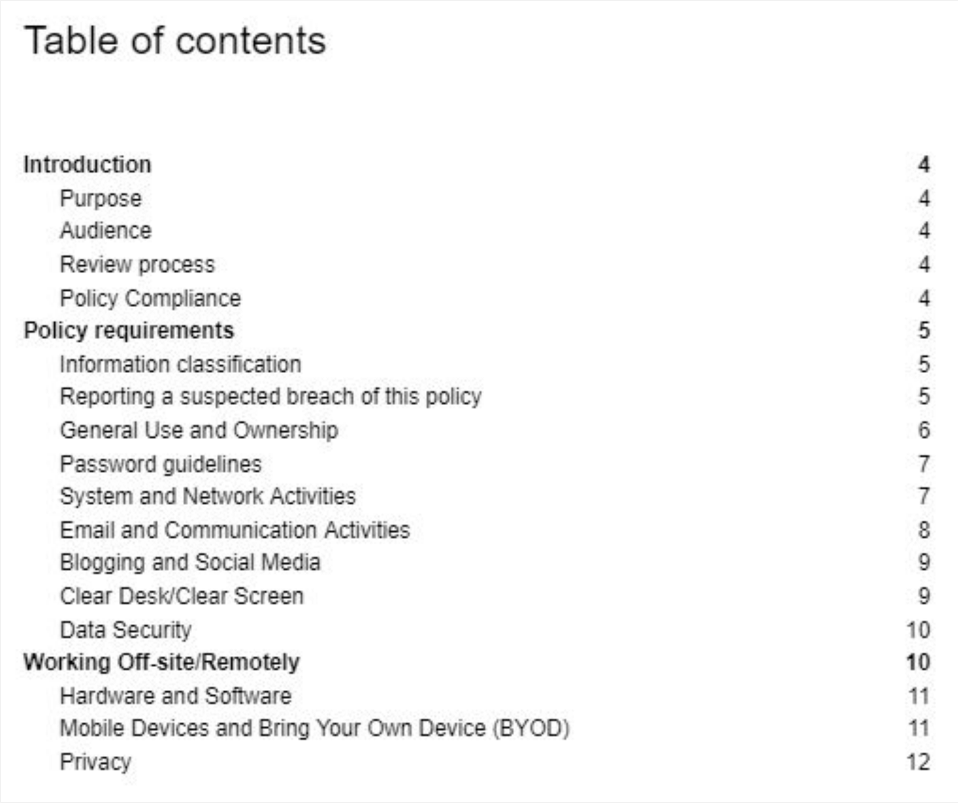


Table of contents

Incident Response Plan

IT incidents can have disastrous consequences, even more so if it is unclear what should happen when confronted with an incident. Unclear communication lines and responsibilities can aggravate the situation and prevent the organisation from learning from less severe incidents. In the document we propose how an organisation can deal with a variety of incidents of various threat levels and overall limit the impact and ensure all stakeholders are informed appropriately (e.g. clients when a database has been breached).

Notes:

- The template plan is aligned with industry best practice and uses the OODA loop decision cycle to focus on filtering available information, putting it in context and quickly making the most appropriate decision.
- The document has unique sections that can and should be amended based on the company's specifics.
- Share the policy with all members of senior management and key members of the IT team.
- Ensure a printed version of this plan is given to the above staff members, in case the network is down and the plan cannot be accessed digitally.
- The security incident response plan should be updated and tested annually to ensure preparations work as designed and can be implemented as smoothly as possible. This can be done via table-top exercises (see here for some examples).

Although primarily written to help organisations deal with IT incidents, this document equally applies to other forms of incidents that require a coordinated approach.

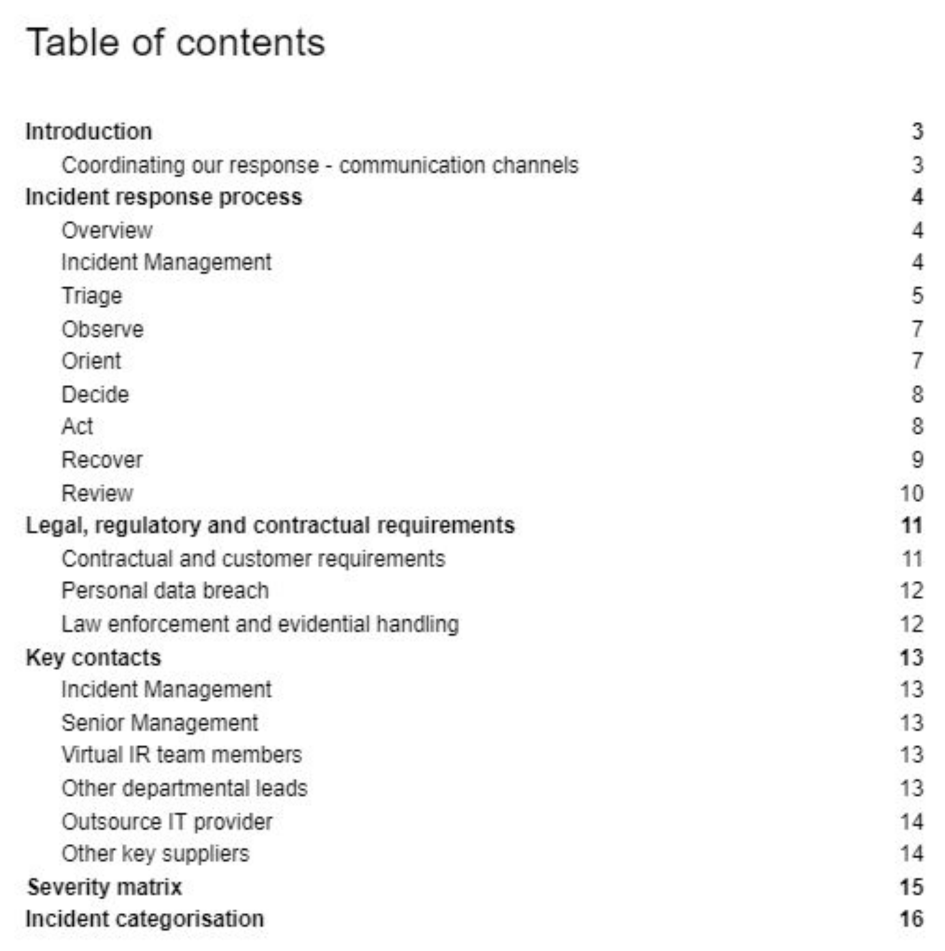


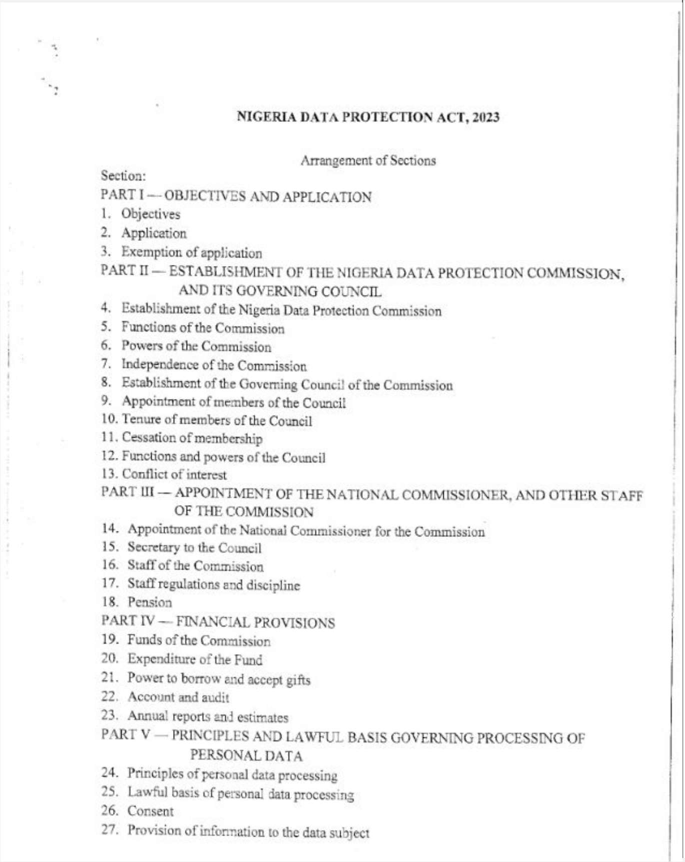
Table of contents

Local Regulations

How to make sure you comply with local regulations?

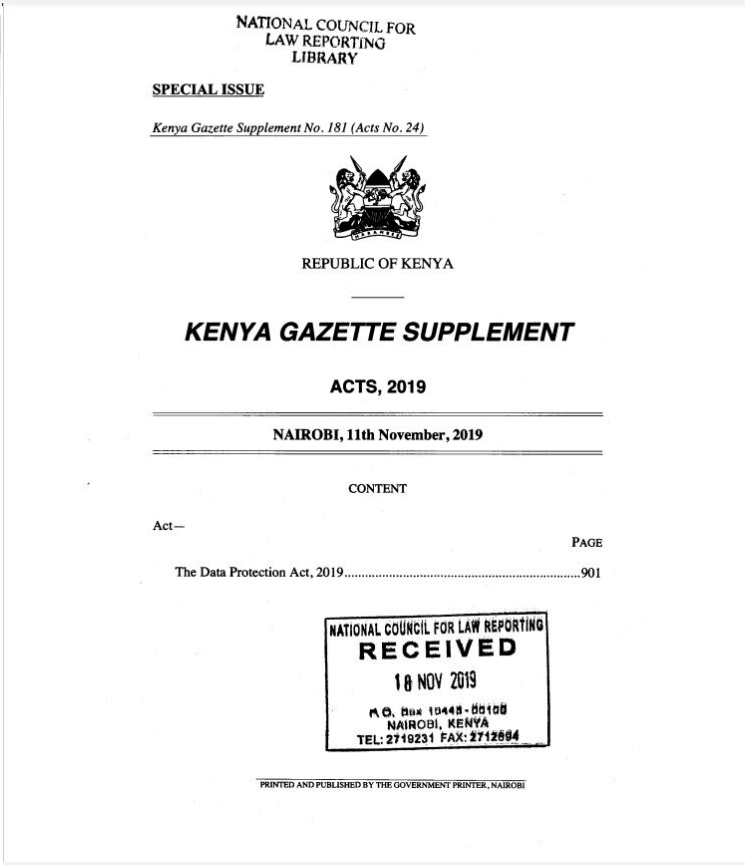
- Aside from the European GDPR , several African countries have also adopted Data security laws. Countries like Kenya, Nigeria and South Africa have adopted laws that help protect its citizens.

- As these vary per country, it is important to identify these regulations and ensure you are compliant



NIGERIA DATA PROTECTION ACT, 2023

Arrangement of Sections



SPECIAL ISSUE

Kenya Gazette Supplement No. 181 (Acts No. 24)

REPUBLIC OF KENYA

KENYA GAZETTE SUPPLEMENT

ACTS, 2019

NAIROBI, 11th November, 2019

CONTENT

PRINTED AND PUBLISHED BY THE GOVERNMENT PRINTER, NAIROBI

Contact

Persistent tech team

+254 769 402 061

security@persistent.energy

Additional information and publications can be found on our website:

www.persistent.energy

PERSISTENT

Triple Jump

Legal Disclaimer

This presentation is being furnished on a confidential basis. No investment is being offered hereby; such investment will only be offered under definitive agreements between Persistent Energy Capital LLC ("Persistent") and the potential investor. No investment in Persistent has been approved or disapproved by the United States Securities and Exchange Commission (the "SEC") or by the securities regulatory authority of any U.S. state or any other country, nor has the SEC or any such securities regulatory authority passed upon the accuracy or adequacy of this presentation. Any representation to the contrary is a criminal offense.

An investment in Persistent will be offered only under an exemption provided by Section 4(a)(2) of the Securities Act and Regulation D promulgated thereunder and other exemptions of similar import in the laws of the states and other countries where the offering will be made. Investments will be offered and sold outside the United States under the exemption provided by Regulation D and/or Regulation S promulgated under the Securities Act. Persistent will not be registered as an investment company under the U.S. Investment Company Act of 1940, as amended (the "Investment Company Act"), in reliance on the exemption provided under Section 3(c)(1) of the Investment Company Act.

An investment in Persistent is suitable only for sophisticated investors and requires the financial ability and willingness to accept the high risks and lack of liquidity inherent in an investment in Persistent. Investors in Persistent must be prepared to bear such risks for an extended period of time and must be prepared to bear the risk of a loss of their entire investment. No assurance can be given that Persistent's operations or investments will generate gain or return capital or that its objectives will be achieved or that investors will receive a return of their capital.

In making an investment decision, investors must rely on their own examination of Persistent and the terms of the offering of an investment, including the merits and risks involved. Prospective investors should not construe the contents of this presentation as legal, tax, investment or accounting advice, and each prospective investor is urged to consult with its own advisors with respect to legal, tax, regulatory, financial and accounting consequences of its investment in Persistent.

This presentation is to be used by the prospective investor to whom it is furnished solely in connection with determining whether it wishes to consider an investment in Persistent. The information contained herein should be treated in a confidential manner and may not be reproduced or used in whole or in part for any other purpose, nor may it be disclosed without the prior written consent of Persistent.

In considering the prior performance information contained in this presentation, prospective investors should bear in mind that past performance is not necessarily indicative of future results, and that there can be no assurance that Persistent will achieve comparable results or that Persistent will be able to make investments similar to the historic investments presented herein because of, among other things, economic conditions, lack of access to capital, changing times and the availability of investment opportunities, and a different investment team.

Although the information contained in this presentation has been obtained from sources deemed by Persistent to be reliable, Persistent makes no representations or warranties regarding the accuracy or completeness of the information and Persistent has not independently verified any such information. The estimates included in this presentation are based upon assumptions that Persistent considers reasonable as of the time made. The estimates are based upon assumptions, all of which are inherently subjective and difficult to predict and many of which are beyond Persistent's control. As a result, the assumptions may not be correct, and the estimates, in turn, may be materially different from actual results and events. There can be no assurance that any estimated returns can be realized or that the actual returns will not be materially lower than those estimated in this presentation. All numbers and information contained in this presentation are unaudited.

The distribution of this presentation and any subsequent offer and sale of an investment in Persistent may be restricted by law in certain jurisdictions. This presentation does not constitute an offer to sell or the solicitation of an offer to buy in any state or other country to any person to whom it is unlawful to make such an offer or solicitation in such state or country. Prospective non-U.S. investors should inform themselves as to the legal requirements and tax consequences within the countries of their citizenship, residence, domicile and place of business with respect to the acquisition, holding or disposal of an investment in Persistent, and any foreign exchange restrictions that may be relevant thereto before considering an investment in Persistent.

Persistent reserves the right, in its sole discretion, to reject an interest by any prospective investor that wishes to consider an investment in Persistent