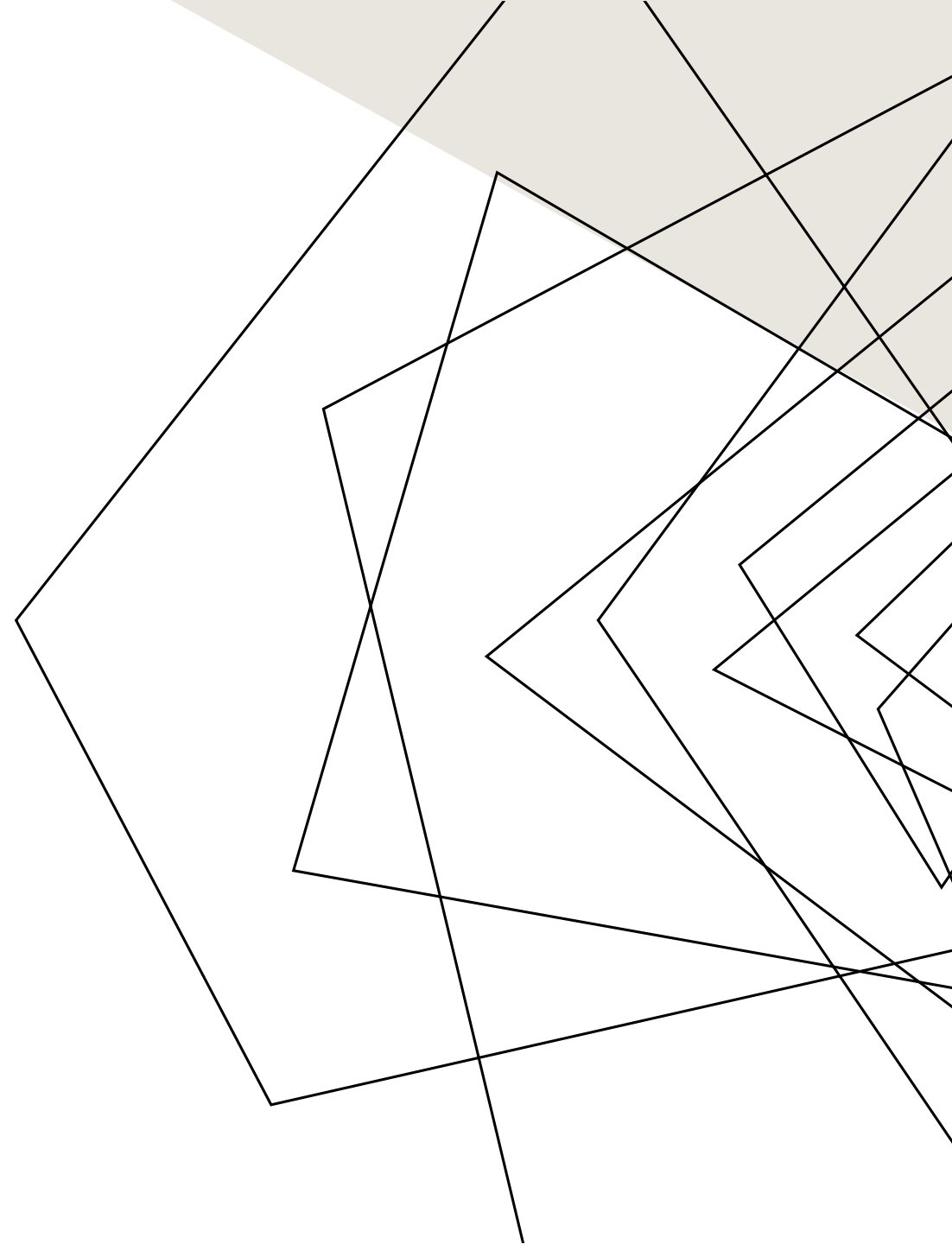


FINSECURE LTD – PROPOSED
COMPREHENSIVE CYBERSECURITY
POLICY AND PLAN
VICTORIA PRICE
2315903
DATA AND INFORMATION SYSTEMS

FINSECURE LTD

Mitigation of internal and external threats is something that should be a focus of any organisation; especially an organisation that mainly deals with sensitive data and financial information.

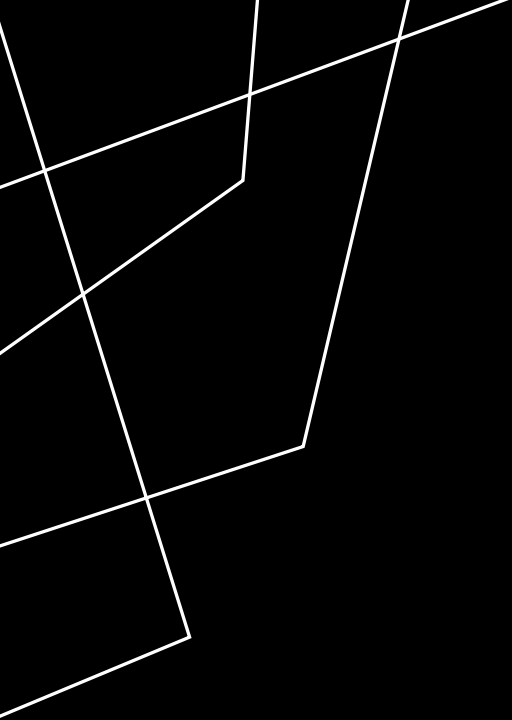


PURPOSE

- Address the recent threats that FinSecure LTD have dealt with.
- Educate on potential threats to the organisation.
- Advise an outline of mitigation measures and policies to implement into the organisation.
- Propose a training plan to ensure adherence to new policies.

GOAL

- The goal of this PowerPoint and report is to educate staff and strengthen the understanding of how vital it is to have strong policies and mitigation procedures.
- Along with this, we want to create a stronger environment for staff to feel comfortable with spotting and reporting potential threats.



POTENTIAL THREATS



INTERNAL THREATS AND EXAMPLES -

Unpatched Systems

- Outdated server systems (e.g. Windows server 2012)
- Web servers
- VPN networks

Insider Trading

- Employees leaking sensitive data for money or other benefits
- Sharing potential professional progresses FinSecure LTD might make
- Unauthorised access to information for the purpose of leaking it

EXTERNAL THREATS AND EXAMPLES -

Phishing and Spear Phishing

- Impersonation of authorised accounts, organisations or people
- Personalised correspondence impersonating trusted entities

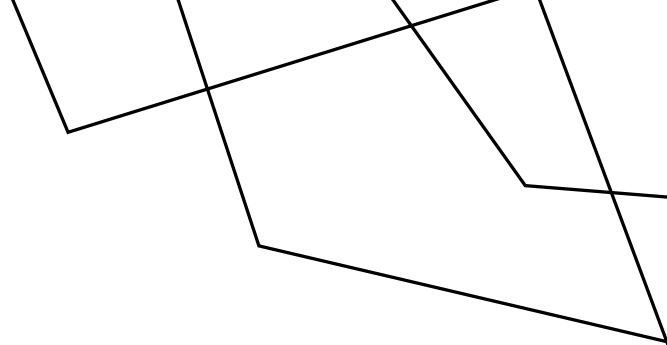
Business Email Compromise

- Spoofed or hacked accounts
- Suspicious requests from trusted entities
- Fake invoices or payment details from trusted entities



REGULATORY BODIES

For organisations to be efficiently protected and secure, they must abide by industry standards.



- **ISO 27001**

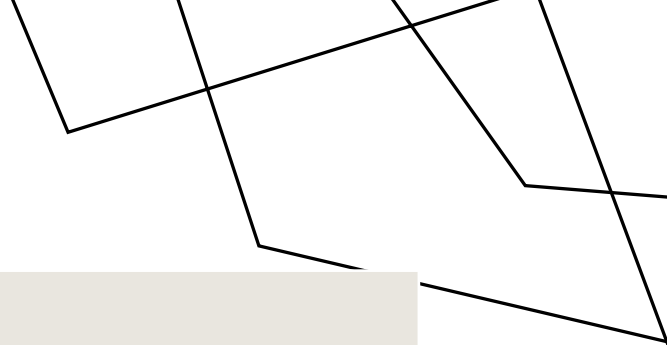
- **GDPR**

- **NIST**

- An international information security standard.
- An EU regulatory body focused on protection of customer's sensitive data.
- The National Institute of Standards and Technology is applicable to all organisations within the US.



IMPLEMENTING POLICIES



Type of Policy	How it will be beneficial
Data Mapping	Minimise the risk of insider leaks and unauthorised access to data
Access Controls	Minimise the risk of insider leaks and unauthorised access to data
Regular Audits	Ensuring all policies are abided by
Incident Reponse and Action	To make the work environment a safe space to raise concerns and to protect sensitive information as efficiently as possible

MITIGATION MEASURES



MITIGATION MEASURES

- **Multi-Factor Authentication (MFA)**
 - Mitigates unauthorised access and phishing
- **Data Encryption**
 - Mitigates data breaches and outsider interception
- **Firewalls**
 - Mitigates unauthorised access
- **Third-Party Management**
 - Mitigates third-party breaches and Man-in-the-Middle attacks



MFA and encryption evidence the usage of the CIA triad when implementing mitigation procedures. This is because they prove that the confidentiality and integrity of data that we hold within the network is incredibly important to the organisation.





STAFF TRAINING AND AWARENESS

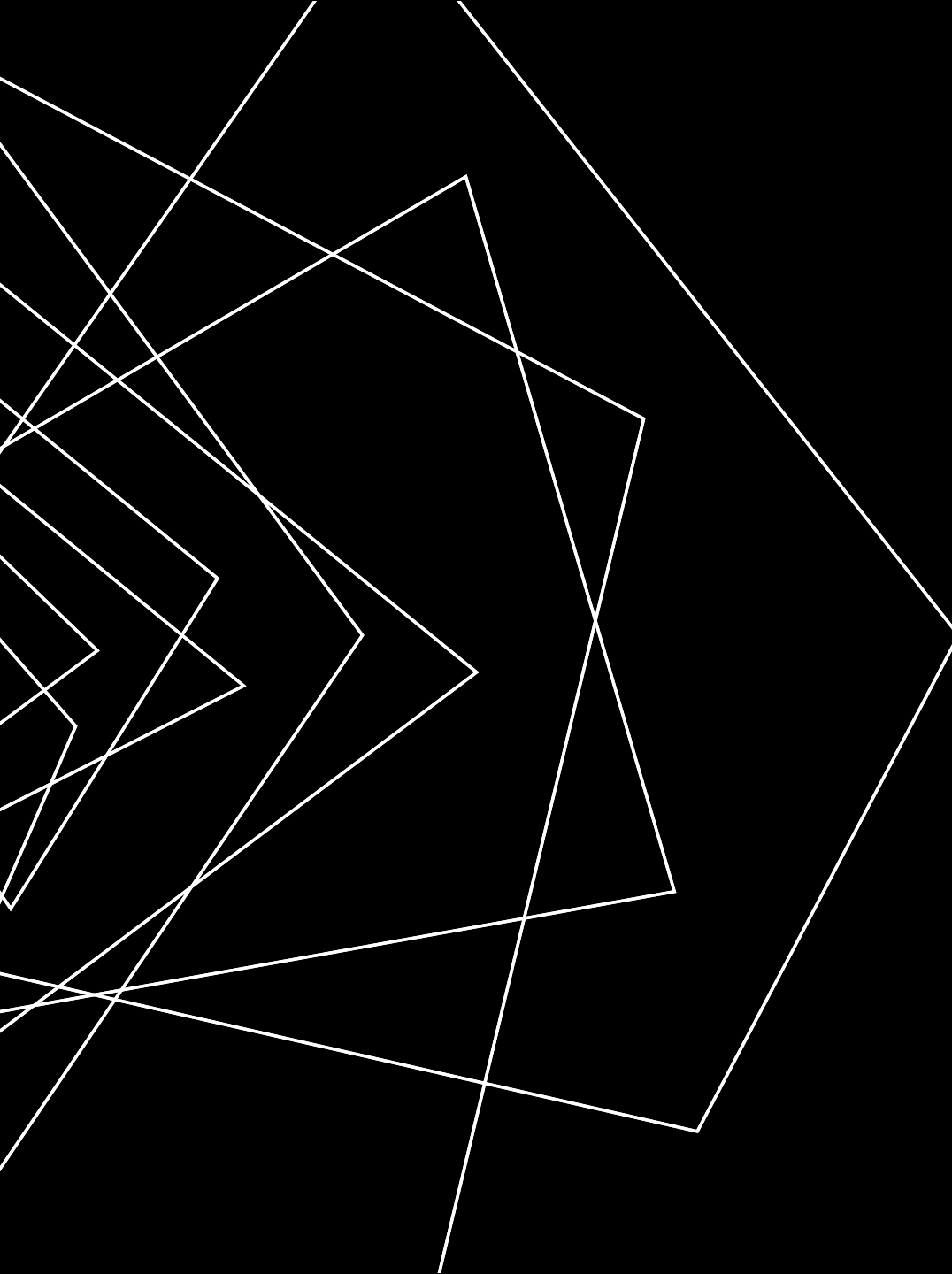
STAFF TRAINING PROPOSED PLAN

- Training program via Teams by a member of the IT Support Team
- Testing of employee understanding by sending simulated fake phishing or BEC correspondence
- Meetings with the IT Support Team if more training is needed
- Drop-In sessions available to staff with the IT Support Team
- Payroll tracking

BENEFITS OF IMPLEMENTING THE PROPOSED PLAN

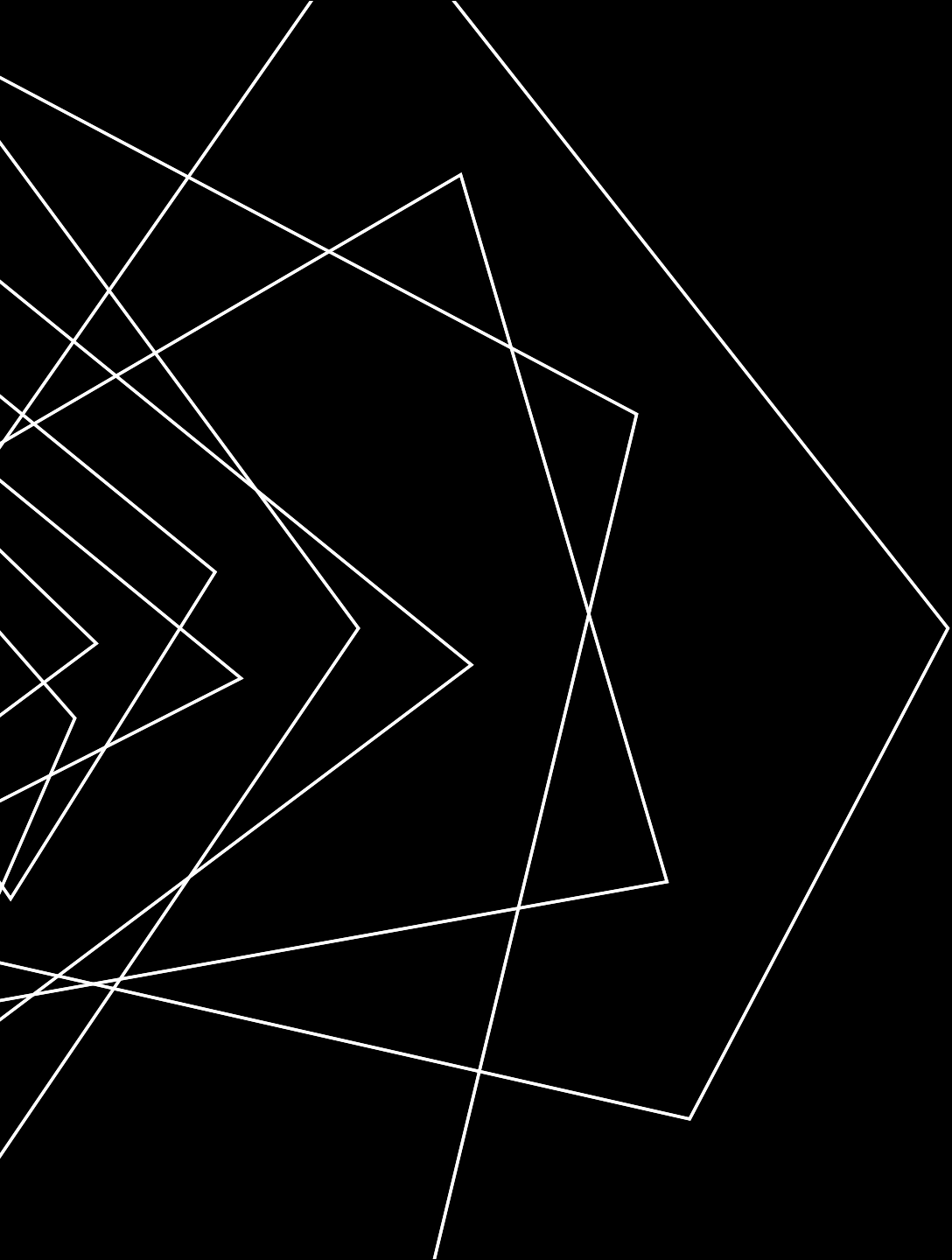
- Improved confidentiality and integrity of sensitive data
- Develop further understanding on staff knowledge
- Improving the reputation of FinSecure LTD
- Ensuring compliance to a multitude of Regulatory Bodies
- Reduce the risk of human error





FINAL RECOMMENDATIONS

- Implement the Training Plan
- Ensure compliance to Regulatory Bodies
- Quarterly reviews of progress to further develop the organisation
- Regular audits to pick-up on any continuous issues or attack to increase or change method of mitigation



THANK YOU FOR YOUR
TIME TODAY.

ANY QUESTIONS?