CYBER SECURITY POLICY

OBJECTIVE

This Cyber Security Policy sets out guidance on how to protect the information assets of Production Concepts Ltd from unauthorised access, data breaches, and other cyber threats. This policy ensures the integrity, confidentiality, and availability of our data and IT systems. This policy applies to all employees, contractors, consultants, and third-party vendors who have access to Production Concepts Ltd.'s IT systems, data, and network infrastructure.

ROLES AND RESPONSIBILITIES

- **Executive Management**: Directors of Production Concepts Ltd will oversee the overall implementation and enforcement of the cybersecurity policy.
- **External IT Security Team**: Manage cybersecurity measures, monitor systems, and respond to incidents.
- **Employees**: Comply with the policy and report any security incidents or vulnerabilities.
- **Third-Party Vendors**: Adhere to the policy when accessing Production Concepts' systems and data.

ACCESS CONTROL

- **Role-Based Access**: Access to systems and data is granted based on their level of authority within the business.
- **Regular Reviews**: Access rights are reviewed quarterly to ensure appropriateness.

SECURE DEVICE USE:

- **Strong Passwords:** Use complex passwords and change them regularly.
- **Two-Factor Authentication (2FA):** Enable 2FA on all accounts that support it.
- **Secure Workstations:** Lock your computer when away and avoid leaving devices unattended.
- **Avoid Public Wi-Fi:** Use a secure connection like a VPN when accessing company resources from public or unsecured networks.

DATA PROTECTION

- **Data Encryption:** Encrypt sensitive data both in transit and at rest.
- **Backup Data:** Regularly back up critical data to secure storage.
- **Data Access:** Only access and share data that is necessary for your role.

NETWORK SECURITY

- **Firewalls and Intrusion Detection**: Firewalls are configured to block unauthorised access, and intrusion detection systems (IDS) monitor network traffic for suspicious activities.
- **Secure Configurations**: Network devices are configured securely following best practices, with unnecessary services disabled.

ENDPOINT SECURITY

- **Anti-Malware**: All endpoints must have up-to-date anti-malware software installed.
- **Patch Management**: Operating systems and applications are regularly updated with security patches.
- **Device Management**: Use of corporate-owned and managed devices for accessing company systems is mandatory.

INCIDENT RESPONSE

- **Incident Reporting**: All cybersecurity incidents must be reported immediately to James Deakin, Project Director, or Greg Deakin, Operations Director.
- **Response Plan**: This will then be escalated to our external IT Security Team who will follow the incident response plan, which includes containment, eradication, recovery, and post-incident analysis.
- **Communication**: Relevant stakeholders will be informed according to the incident communication plan.

USER BEHAVIOR

- **Acceptable Use**: Company IT resources are to be used for business purposes only. Personal use is limited and must not interfere with work responsibilities or security.
- **Phishing Awareness**: Employees must be trained to recognize and report phishing attempts.
- **Remote Work**: Remote access must be secured via a VPN and adhere to the same security standards as on-site access.

RESPONSIBLE USE OF SOCIAL MEDIA:

- **Limit Information Sharing:** Avoid sharing sensitive company information or details about your role and workplace on social media.
- **Privacy Settings:** Use strong privacy settings to protect personal information.

TRAINING AND AWARENESS

- **Mandatory Training**: All employees must complete annual cybersecurity training.
- **Ongoing Education**: Regular updates and refresher sessions on cybersecurity best practices will be provided.

COMPLIANCE

- **Regulatory Compliance**: Production Concepts Ltd will comply with all applicable laws and regulations where relevant.
- **Internal Audits**: Periodic audits will be conducted to ensure adherence to this policy.

MONITORING AND AUDITING

- **Continuous Monitoring**: Systems and networks are continuously monitored for potential security threats via an external IT company.
- **Audit Logs**: Logs of system and network activities are maintained and reviewed regularly.

POLICY REVIEW AND UPDATES

- **Regular Reviews**: This policy will be reviewed and updated annually or as needed to address new threats or changes in technology.
- **Approval**: Changes to this policy require approval from the Executive Management.

POLICY ACKNOWLEDGMENT

- All employees, contractors, and third-party vendors must acknowledge their understanding and acceptance of this policy upon onboarding and whenever significant changes are made.

them but as email is the most likely source of an attack you need a strategy for dealing with malicious emails and generally improving your email security.

It can take as little as 1 minute 29 seconds for an organisation to be breached by a phishing attack, with over 22 percent of employees falling victim.

The consequences of a successful attack could be catastrophic if information is leaked, financially, and operationally, and your business' reputation will be harmed.

There are several security measures you can take which will reduce the risk of malicious emails getting through or - if anyone does click on them – to minimise the damage caused.

Authorised

This policy will be reviewed and updated annually by senior management.

Review Date: May 2025

Position	Print Name	Signature	Date
Company Director	James Deakin		**31/05/24**
Company Director	Greg Deakin		**31/05/24**
Company Director	Stefan Chadwick		**31/05/24**