deepalert

ALWAYS LOOKING OUT FOR YOU

DeepAlert Cyber Security Policy

Version	Description	Date	Author
1.0	Cyber Security Policy	19 November 2020	E Kippie

Scope

This document lays out the DeepAlert Information Security Policy as applicable to all employees and contractors.

Background

DeepAlert deals extensively with customer data in the form of camera images, configurations and customer personal and organisational information and, in addition, has a significant body of its own IP. It is therefore critical to the business that a well defined, clear and well executed security policy is in place which applies to all employees and contractors of the business.

General Principle on System and Data Access

The overarching policy around access to systems and data is that access should only be granted by authorised personnel to others where such access is strongly required in order to perform the official work function of the other. Access and data should exist for only as long as that work function is required and be revoked / destroyed at the end of the work function period.

Data confidentiality is an incredibly important part of our business. All employees are obliged to protect the data of the business. In this policy, we will give our employees instructions on how to avoid data and systems security breaches.

Personal and company devices

Devices used to access the company systems and accounts need to have been approved with the company required security measures in place on the device according to the type of access.

Essential controls for accessing the company systems:

- Ensure Multi Factor Authentication is enabled for specified systems as dictated by company policy.
- Technical access to production systems is strictly controlled.
- Effective antivirus protection should be in place on user devices.
- User devices should not be left exposed or unattended.
- All access to company accounts and systems is through secure connections.

Password Management

Password leaks can compromise the security of our systems. Not only should passwords be secured at all times and be of sufficient complexity so as not to be susceptible to hacking attacks or guesswork.

Employees must follow the following guidelines when managing passwords:

- Root or Systems Administrator passwords and ssh keys are only shared with senior and competent members of the IT department who require these privileges.
- Passwords must not be shared with anyone.
- System passwords should not be saved on mobile phones or sticky notes.
- Use challenging alpha-numeric passwords including special characters.
- Use company approved password manager software to avoid having to remember a large number of passwords

Data Security

- Data is securely stored and accessed from centrally controlled systems with sufficient backups and snapshot capabilities in place.
- Client data is stored in secure ways such that each client's data is segmented from any other client data.

- Data should only be shared following the business processes and systems that have been put in place. Data must not be shared through public chat groups or social media platforms such as WhatsApp, Facebook or Instagram.

- Access to all data is strictly controlled. Access permissions that are sufficient to perform the work function should be applied, and not more permissive. User activity in sensitive areas is logged for audit purposes.

- Intrusion tests are periodically performed on the systems.

All data mishandlings must be reported to our cyber security team immediately.

Email Confidentiality

Emails often host scams and malicious software (e.g. worms.). To avoid virus infections or data theft, we instruct employees to take extra care in this area with the following guidelines:

- Identify “Phishing Emails” and to avoid opening attachments on such emails.

- Phishing emails and text messages often look like they’re from a company you know or trust. Thus even recognizable emails should be given proper scrutiny.

- Be mindful of eye catching subject lines e.g. offerings or prizes.

- Look for inconsistencies or give-aways (e.g. grammar mistakes, capitalization errors or excessive number of exclamation marks).

If an employee isn't sure that an email they receive is safe, they should refer to our cyber security team for advice.

Additional measures for employees

- Turn off screens or lock devices when leaving your desk.

- Report stolen or damaged equipment to HR as soon as possible.

- Change all account passwords and security keys should a device be stolen.

- Report potential system threats or weaknesses in the business systems.

- Avoid accessing suspicious websites and refrain from downloading unauthorized or illegal software or copyright material.

Remote Access

There are no special guidelines for remote access since that is the norm these days for all employees. However, extra vigilance should be taken with any kind of remote work on unsecured networks.

DeepAlert security measures

- Regular checks as signed off by senior management that all physical and digital security measures have been implemented to protect customer data, company data and systems.

- Installation and management of firewalls, anti malware software and access via authenticated systems.

- Cyber security training and awareness sessions for all employees.

- Thorough investigation of any possible security breaches.

- Strict following of the security policies of the business at all times.

Summary

This policy is required to be adopted by all employees and contractors with access to systems and a culture of taking security seriously should be enforced and monitored.

Our customers should feel confident that their data will be stored safely and managed in a controlled and highly secured environment.