CYBER-EXTORTION & BLACKMAIL POLICY

Policy Statement

Cybercrime poses a risk to HR Staff n' Stuff and its employees as it can cause significant loss and have devastating impacts on both the business and the individual involved. Employees are the first and last line of defence against cybersecurity threats. This policy aims to inform and support employees to report any cybercrime, and this policy specifically relates to those resulting in any form of extortion or blackmail.

This policy applies to all HR Staff n' Stuff employees.

Guidelines

1. What is Extortion?

Extortion is a criminal offense of obtaining money, property, or services from an individual or institution, through coercion. Extortion is commonly practiced by organised crime groups. The actual obtainment of money or property is not required to commit the offense. Making a threat of violence which refers to a requirement of a payment of money or property to halt future violence is sufficient to commit the offense. Cyber extortion is an online form of extortion where cyber criminals threaten to disable operations of a business or compromise confidential data unless their demands are met.

2. What is Blackmail?

Blackmail, which always involves extortion, involves the extortionist threatening to reveal information about a victim or their family members that is potentially embarrassing, socially damaging, or incriminating unless a demand for money, property, or services is met.

Some forms of cyber blackmail scams include ransom emails that threaten to distribute compromising images or videos of the recipient unless money is paid, often by cryptocurrencies (virtual or digital money) such as Bitcoin. The scammer may claim to have hacked the person's computer and obtained webcam footage of them looking at adult material, or in some cases the scammer may have actual images or videos of the person, such as material shared as part of an online romance scam.

3. **Other forms of cyber threats** that may result in extortion or blackmail include:

- Malicious software to access personal information or spy on a user's computer to obtain data.
- Phishing emails, messages, or calls or trick the recipient into revealing personal data and giving remote access.
- Ransomware to lock or encrypt files so that they can no longer be used or accessed.

- Impersonation of employees to access money or data through email, phone calls or text messages.

4. Reporting extortion, blackmail, or other cyber threats

Employees must notify and discuss with their Director any unusual or non-standard requests, from both internal and external sources, that require them to spend money and/or provide credentials or other sensitive data.

Employees who believe they may have fallen victim to extortion or blackmail in the workplace are requested to follow the instructions below:

a) Speak to their Director as soon as they become aware of being extorted, blackmailed or any other form of cyber threat.
b) HR Staff n' Stuff Director will notify the appropriate authorities. Any information provided by the affected employee regarding the matter will remain confidential and only communicated to key personnel for the purposes of investigating, managing, and mitigating the threat.
c) Employees must keep any evidence of the cybercrime to maximise forensic investigation of the matter.
d) HR Staff n' Stuff Director, with the cooperation of the employee, will report the incident to appropriate authorities including police and the Australian Cyber Security Centre.

5. Failure to report and comply with this policy

a) If employees fail to comply with this policy, resulting in business funds being used and extorted, they will be personally responsible to repay HR Staff n' Stuff for the full sum. Alternatively, if an employee uses their own funds to make a purchase without first verifying the request's authenticity, then HR Staff n' Stuff will not be liable for reimbursing the employee.

b) If employees fail to comply with this policy, resulting in loss or theft of business data, the matter will be investigated by the Director (this may also include appropriate authorities including police) and the employee may be subject to disciplinary action.