CLC The Specialist Property Law Regulator

Cybercrime Policy Example

'IMPORTANT'

As a business, we are committed to working to minimise the risks posed by Cybercrime and Cyber-terrorism to our clients, third parties and the business. We are a risk because on a daily basis we:

- Hold large sums of monies
- Multiple access points (email, phone etc)
- Third party interactions
- Clients expect speedy transactions

1. As a business, we will manage the risk posed by our IT system by:

   - Install firewalls on our IT systems
   - Keep anti-virus and anti-spyware software up-to-date
   - Create a protocol for Strong passwords
   - Use encryption to protect information contained in e-mails or stored on laptops or other portable devices
   - Destroy old computers, backup drives, memory sticks, etc. using specialist 'shredding' applications or the services of a reliable contractor
   - Clear out temporary internet files, cache and history files (also monitor third-party cookies)
   - Back-up multiple copies of our essential data

2. As a Business, we will prepare a 'Response Plan' covering the internal procedures the business (or an accountable person) must put in place following a potential cyberattack. The Response Plan will focus on protecting the interest of our clients and third parties, and to provide a contingency process to manage the business.

3. We must at all times take steps to ensure that our business is not unintentionally open to a cyber attack and will develop practical safeguards to protect our clients, third parties and the business in the below areas:

   - Email interception
   - Ransom Ware

- Creating fake offices
- Cashier and SDLT payments
- Phone calls from banks
- Emails from practices
- Hacking of accounting systems

4. We must explain to clients the need to protect ourselves and them from cybercrime and make them aware of the practical steps they can take to protect themselves and inform them t either in our terms of engagement or otherwise in writing.

5. We will ensure that staff are given appropriate and regular training to create a culture of 'prevention' on two level.

5.1 'User' Level Prevention Steps

Front line staff, including receptionist and administrator, case handlers, will be trained to ensure that they:

- are certain that a phone call is from our, clients bank, or a parties bank;
- receive a call from a 'bank' they should use a different phone to call the bank back and ask to speak to the firms relationship/business manager, or designated named individual;
- never disclose passwords on phone/by email;
- never allow a 3rd party access to systems remotely;
- know that we will never inform clients or third parties about any change of bank details; unless in an exceptional circumstance when this will be done in writing by post.

5.2 'Senior Personnel/Business' Level Prevention Steps

HoLP/HoFA, directors, partners, members and owners, will ensure that the Business operates the following types of mitigation to help the business manage the technological risks associated to Cybercrime and Cyber-terrorism.

- Put in place a IT protocol to include a hierarchy of user privileges – restricted data access;
- Maintain effective and current Software support;
- Ensure the business is running with upto-date antivirus and antimalware
- Put in place strict guidance for remote working , for example not using unsecure WI-FI access available in public areas, such as train stations and coffee shops etc
- Monitoring use of inappropriate websites, social media and when necessary blocking access;
- Put in place staff guidance to manage the consequences of any breach of information security violations – including, where necessary disciplinary policy;
- Swiftly, removing access rights of staff who have left and closing redundant accounts.

6. As a Business, we will ensure ALL senior personnel know who to notify in the event of a Cybercrime or incident, including but not limited to:

    - Action Fraud – National Fraud and Cybercrime Reporting Unit
    - Our staff
    - Our Clients
    - ICO
    - Our Professional indemnity insurer
    - The relevant Banks, mortgage lenders, accountants, or parties that may have been affected.
    - The CLC

7. As a Business, if we suspect that we have a problem with our cybersecurity, or could be the victim of cybercrime, or are simply concerned that we may have been; we will recognise that **we MAY NOT be the ONLY victim** and will take immediate steps to **help protect our regulated community by informing the CLC**.

Useful Links

Cyber Essentials: https://www.cyberstreetwise.com/cyberessentials/

IASME: https://www.iasme.co.uk/index.php

SRA Cybercrime Report: http://www.sra.org.uk/documents/solicitors/freedom-in-practice/cybercrime.pdf

Action Fraud: http://www.actionfraud.police.uk/