CYBER SECURITY POLICY OF INDEPENDENT BOARD EVALUATION

1. BACKGROUND

Our company cyber security policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure.

We have implemented a number of security measures and prepared instructions that may help mitigate security risks. We have outlined both provisions in this policy. This policy applies to all our employees or contractors who have permanent or temporary access to our systems and hardware.

Our Office 365 System ("SharePoint") is our cloud technology system for working together and for gathering and sending data to IBE colleagues. Our IT specialists keep the system up to date and are responsible for installing the latest protective software on our devices.

2. POLICY ELEMENTS

All employees are obliged to protect confidential data such as Unpublished financial information, Data of customers/partners/vendors, Customer lists (existing and prospective), interview notes and draft and final reports and we have given our employees instructions on how to avoid security breaches which follow:

2.1. PROTECT PERSONAL AND COMPANY DEVICES

We advise our employees to keep both their personal and company-issued computer, tablet and cell phone secure. They have been advised to:

- Keep all devices password protected.
- Choose and upgrade a complete antivirus software.
- Ensure devices are not left exposed or unattended.
- Install security updates of browsers and systems monthly or as soon as updates are available.
- Log into company accounts and systems through secure and private networks only.

Employees are advised to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

All company-issued equipment or equipment used for the purposes of our work will have:

- Disk encryption setup
- Antivirus/ anti-malware software

Employees/contractors should follow instructions to protect their devices and refer to our IT specialists if they have any questions.

2.2. KEEP EMAILS SAFE

To avoid virus infection or data theft, we instruct employees to:

- Avoid opening attachments and clicking on links when the content is not adequately explained or expected.
- Be suspicious of clickbait titles (e.g. offering prizes, advice.)
- Check email and names of people they receive a message from to ensure they are legitimate.

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

If an employee isn't sure that an email they received is safe, they can refer to our IT specialists.

2.3. MANAGE PASSWORDS PROPERLY

We advise our employees to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays.)
- Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
- Exchange credentials only when absolutely necessary. When exchanging them in-person isn't possible, employees should prefer the phone instead of email, and only if they personally recognise the person they are talking to.

2.4. TRANSFER DATA SECURELY

Transferring data introduces security risk. Employees must:

- Avoid transferring sensitive data to other devices or accounts unless absolutely necessary.
- Share confidential data over the company network/ system and not over public Wi-Fi or private connection.
- Ensure that the recipients of the data are properly authorised people or organisations and have adequate security policies.
- Report scams, privacy breaches and hacking attempts to our IT specialists, who will investigate promptly.

We encourage our employees to contact our IT specialists with any questions or concerns.

2.5. ADDITIONAL MEASURES

To reduce the likelihood of security breaches, we also instruct our employees to:

- Turn off their screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible to our IT specialists.
- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in company systems.
- Refrain from downloading suspicious, unauthorised or illegal software on their company equipment.
- Avoid accessing suspicious websites.
- Install firewalls, anti malware software and access authentication systems.
- Arrange for security training to all employees.
- Inform employees regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.

3. DISCIPLINARY ACTION

We expect all our employees to always follow this policy and those who cause security breaches may face disciplinary action:

- First-time, unintentional, small-scale security breach: We may issue a verbal warning and train the employee on security.
- Intentional, repeated or large-scale breaches (which cause severe financial or other damage): We will invoke more severe disciplinary action up to and including termination.
- We will examine each incident on a case-by-case basis.

Additionally, employees who are observed to disregard our security instructions will face progressive discipline, even if their behaviour hasn't resulted in a security breach.