GROUP POLICIES AND GUIDELINES

Information Technology

This employee internet usage policy applies to our employees, contractors, volunteers and partners who have access to our network and computers. Employees are advised to use the office's internet for the following reasons:

- To complete their job duties;
- To seek out information that they can use to improve their work;
- To access their social media accounts, while conforming to our social media policy.

While the Yoma Group does not want to restrict our employees' access to websites of their choice, but we expect our employees to exercise good judgment and remain productive at work while using the internet. Any use of our network and connection must follow our confidentiality and data protection policy.

Employees should:

- Keep their passwords secret at all times;
- Log into their corporate accounts only from safe devices;
- Use strong passwords to log into work-related websites and services.

Employees should not use the network to:

- Download or upload obscene, offensive or illegal material;
- Send confidential information to unauthorized recipients;
- Invade another person's privacy and sensitive information;
- Download or upload movies, music and other copyrighted material and software;
- Visit potentially dangerous websites that can compromise the safety of our network and computers;
- Perform unauthorized or illegal actions, like hacking, fraud, buying/selling illegal goods and more.

Employees are advised to be careful when downloading and opening/executing files and software. If they're unsure if a file is safe, they should ask their supervisor or IT helpdesk. Anti-virus and disk encryption software may be installed on the Yoma Group's computers. Employees may not deactivate or configure settings and firewalls without managerial approval. The Yoma Group shall not be responsible if employee devices are infected by malicious software, or if their personal data are compromised as a result of inappropriate employee use.

Company-issued Equipment

Employees are expected to respect and protect any equipment belonging to the Yoma Group. "Company equipment" in this computer usage policy for employees includes company-issued phones, laptops, tablets and any other electronic equipment, and belongs to our company. Employees are also advised to lock their devices in their desks when they're not using them and remain responsible for their any Company equipment whenever taken out of the offices.

Employees may use their corporate email accounts for both work-related and personal purposes as long as they don't violate this policy's rules. Employees shouldn't use their corporate email to:

- Register to illegal, unsafe, disreputable or suspect websites and services;
- Send obscene, offensive or discriminatory messages and content;
- Send unauthorized advertisements or solicitation emails;
- Sign up for a competitor's services unless authorized;

The Yoma Group has the right to monitor corporate emails. And the right to monitor websites employees visit on any Company equipment.

Disciplinary Action

Employees who do not comply with this employee internet usage policy will face disciplinary action. Serious violations will be cause for termination of employment, or legal action when appropriate. Examples of serious violations are:

- Using our internet connection to steal or engage in other illegal activities.
- Causing our computers to be infected by viruses, worms or other malicious software.
- Sending offensive or inappropriate emails to our customers, colleagues or partners.

Employee Social Media Policy

The Yoma Group's social media policy provides a framework for using social media. Social media is a place where people exchange information, opinions and experiences to learn, develop and have fun. Whether employees are handling a corporate account or use one of their own, they should remain productive. The Yoma Group will differentiate between an employee's use of personal social media at work and the use of corporate accounts as may be required in the performance of the duties. This policy provides practical advice to avoid issues that might arise by careless use of social media in the workplace. All employees are expected to follow this policy.

"Social media" refers to a variety of online communities like blogs, social networks, chat rooms and forums. This policy covers all of them. Employees are advised to:

- Use their common sense. If employees neglect their job duties to spend time on social media, their decline in productivity will show on their performance reviews.
- Ensure others know that personal account or statements don't represent our company. Employees shouldn't state or imply that their personal opinions and content are authorized or endorsed by our company. We advise using a disclaimer such as "opinions are my own" to avoid misunderstandings.
- Avoid sharing intellectual property like trademarks on a personal account without approval. Confidentiality policies and laws always apply.
- Avoid any defamatory, offensive or derogatory content. It may be considered as a violation of our company's anti-harassment policy, if directed towards colleagues, clients or partners.
- Avoid posting any material that: (i) constitutes harassment, hate speech, or libel; (ii) violates the privacy rights of fellow employees; or (iii) is disruptive to the work environment because it impairs workplace discipline or control, impairs or erodes working relationships, creates dissension among co-workers, interferes with job performance, or obstructs operations.

Representing our company

Some employees represent our company by handling corporate social media accounts or speak on our company's behalf. We expect them to act carefully and responsibly to protect our company's image and reputation. Employees should:

- Be respectful, polite and patient, when engaging in conversations on our company's behalf. They should be extra careful when making declarations or promises towards customers and stakeholders;
- Avoid speaking on matters outside their field of expertise when possible. Everyone should be careful not to answer questions or make statements that fall under somebody else's responsibility;
- Follow our (9.2.2) Confidentiality Policy and (9.2.3) Data Protection Policy; and observe laws on copyright, trademarks, plagiarism and fair use;
- Inform our Group Communications or relevant Marketing department when they're about to share any impactful content;
- Avoid deleting or ignoring comments for no reason. They should listen and reply to criticism;
- Never post discriminatory, offensive or libelous content and commentary;
- Correct or remove any misleading or false content as quickly as possible

Disciplinary Consequences

The Yoma Group will monitor all social media postings on its corporate account. Disciplinary action may be taken if employees do not follow this policy's guidelines. Examples of non-conformity with the employee social media policy include but are not limited to:

- Disregarding job responsibilities and deadlines to use social media
- Disclosing confidential information through personal or corporate accounts
- Directing offensive comments towards other members of the online community

Employee confidentiality policy on Disclosure of Official Documents, Information and Trade Secrets

All documents, papers and information acquired in an employee's official capacity or otherwise should be treated as confidential and trade secrets of the Yoma Group. Employees must not copy, reproduce, extract, translate or in any way deal with them in a manner that is not authorized or allow others to do so, or disclose, publish or communicate them to the Press or to individuals whether directly or indirectly unless it is in the course of their official duties or if it is lawfully required or authorized by any Court of law or with authorization from the Management. This clause shall continue to apply even after they are no longer employed by the Yoma Group.

This policy affects all employees, including board members, investors, contractors and volunteers, who may have access to confidential information. Confidential and proprietary information is secret, valuable, expensive and/or easily replicated. Common examples of confidential information are:

- Unpublished financial information;
- Data of Customers/Partners/Vendors;
- Patents, formulas or new technologies;
- Customer lists (existing and prospective);

- Data entrusted to our company by external parties;
- Pricing/marketing and other undisclosed strategies;
- Documents and processes explicitly marked as confidential;
- Unpublished goals, forecasts and initiatives marked as confidential.

Employees may have various levels of authorized access to confidential information. What employees should do:

- Lock or secure confidential information at all times;
- Shred confidential documents when they're no longer needed;
- Make sure they only view confidential information on secure devices;
- Only disclose information to other employees when it's necessary and authorized;
- Keep confidential documents within the Yoma Group's premises unless it's absolutely necessary to remove them.

What employees shouldn't do:

- Use confidential information for any personal benefit or profit;
- Disclose confidential information to anyone outside of our company;
- Replicate confidential documents of the Yoma Group's files and store them in unsecured devices upon termination or expiry of the employee's employment with the Yoma Group, employees are obliged to return any confidential files and delete them from their personal devices.

Confidentiality Measures

The Yoma Group takes measures to ensure that confidential information is well protected, including but not limited to:

- Storing and locking paper documents;
- Encrypting electronic information and safeguarding databases;
- Requiring employees to sign non-compete and/or non-disclosure agreements (NDAs);
- Requesting for authorization by senior management to allow employees to access certain confidential information.

Exceptions are:

- Confidential information may occasionally have to be disclosed for legitimate reasons. Examples are: If a regulatory body requests it as part of an investigation or audit;
- If our company examines a venture or partnership that requires disclosing some information (within legal boundaries).

In such cases, employees involved should document their disclosure procedure and collect all needed authorizations; and should not disclose more information than required.

Disciplinary Consequences

Every breach of the confidentiality policy will be investigated. Employees who do not comply with the confidentiality policy will face disciplinary and possibly, legal action. In the event that any employee willfully or regularly breaches the confidentiality policies for personal benefit, the Yoma Group reserve

the right to terminate the employment of such employee immediately. This policy is binding even after termination or expiry separation of employment.

Company Data Protection Policy

This policy is applicable to all parties (including employees, job applicants, customers, suppliers, contractors etc.) who provide information to the Yoma Group. As part of our operations, the Yoma Group may need to obtain and process information. This information includes any offline or online data that makes a person identifiable such as names, addresses, usernames and passwords, digital footprints, photographs, social security numbers, financial data etc. The Yoma Group will collect this information in a transparent manner and with the full cooperation and knowledge of interested parties. The Yoma Group will ensure that the personal data be:

- Collected fairly and for lawful purposes only;
- Processed by the company within its legal and moral boundaries;
- Protected against any unauthorized or illegal access by internal or external parties.

Any personal data will not be:

- Communicated informally;
- Stored for more than a specified amount of time;
- Transferred to organizations, states or countries that do not have adequate data protection policies Distributed to any party other than the ones agreed upon by the data's owner (exempting legitimate requests from law enforcement authorities)

During the collection process of personal information, the Yoma Group also undertakes to:

- inform people that their data is collected;
- Inform people about how data is processed;
- Have provisions in case of lost, corrupted or compromised data;
- Allow people to request that any data provided in relation to themselves be modified, erased, reduced or corrected in the databases.

Actions

The Yoma Group will:

- Restrict and monitor access to sensitive data;
- Develop transparent data collection procedures;
- Train employees in online privacy and security measures;
- Build secure networks to protect online data from cyberattacks;
- Establish clear procedures for reporting privacy breaches or data misuse;
- Include contract clauses or communicate statements on how we handle data;
- Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization etc.)

Disciplinary Consequences

All principles described in this policy must be strictly followed. A breach of data protection guidelines will invoke disciplinary and possibly legal action.