Acceptable Use Policy

March 2025

Version Control and Approval

Version	**001**
Document number	**IT_AUP_01**
Prepared by	**Ingo Hofmaier**
Approved by	**Chris Showalter** 
Approval date	**03 March 2025**
Review period (months)	**03 September 2025**

VERSION HISTORY			
Ver. #	**Ver. Date**	**Revised By**	**Description of Revision**

001	03/03/2025	Ingo Hofmaier	Initial release

Contents

1. Overview

Lifezone Metals Limited and its group of companies ("**Lifezone"** or the "**Company"**) publishes this Acceptable Use Policy not to impose restrictions on its employees, contractors, consultants or suppliers that use any platform, software or system which is licensed owned or operated by Lifezone ("**User"**), but to protect Lifezone's Users (including such employees, contractors and third-party service providers who have access to our systems and information), partners and the Company itself from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet, intranet, extranet-related information systems and assets, including but not limited to computer equipment, mobile devices, software, operating systems, storage media and network accounts providing system, electronic mail and web browsing access are the property of Lifezone. These systems are to be used for business purposes in serving the interests of the Company, and of our clients and customers during normal operations.

Effective information security is a team effort involving the participation and support of every Lifezone User who deals with information, data and/or information systems. It is the responsibility of every User to know these guidelines, and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment, other electronic devices and our information technology assets at Lifezone. These rules are in place to protect employees and contractors and the company. Inappropriate use exposes the company to data loss, cyber risks, including virus and ransomware attacks, compromise of network systems and services, that can lead to data breaches and legal and financial consequences.

3. Scope

This policy applies to the use of Lifezone information systems and assets, including electronic and computing devices, and network resources to conduct Lifezone business, interact with internal networks and systems and web applications, whether owned or leased by Lifezone, the User, or a third party.

Every User (including employees, contractors and third-party service providers who have access to our systems and information) at Lifezone and its subsidiaries is responsible for exercising good judgment regarding appropriate use of information systems and assets, including electronic and computing devices, and network resources in accordance with Lifezone policies and standards, and local laws and regulation.

This policy applies to all Lifezone Users (including employees, contractors and third-party service providers who have access to our systems and information), including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Lifezone.

4. Policy Elements

4.1. Choosing a strong password

- Only use system level and user level passwords that comply with the Password Policy (see the Information Security Policy)
- Don't write down your password – either on paper or on a computer file.
- Don't share your password with colleagues or friends.
- Don't give your password to anyone pretending or saying they are from tech support, via e-mails or over the phone.
  - It is usually a scam and will not be needed if there is a legitimate need to manage your accounts.
- Do consider using a passphrase – a selection of random words, which is easier to remember and may be faster to type than a 'complex' password.
- Don't iterate on your passwords when the system requests a change – e.g., changing from 'Password1' to 'Password2'.
- Don't use personal or work-related words in your password, which someone could trivially guess – no pet names, dates of birth or work project names.
- Do handle your password as if it were something valuable, such as a credit card PIN or a personal secret.
- Don't re-use passwords between systems, and especially not between Lifezone and personal systems – e.g. do not choose the same password to log into your work device and private applications, like LinkedIn, Facebook or Instagram.
- Do consider using a password manager to generate and store complex passwords, but only when you feel confident in managing these tools.
- If in doubt or if you have questions, contact IT management under:
  - *itsupport@lifezonemetals.com*
  - *itsupport@kabanganickel.com*

Do report any loss of password or suspicious activity immediately and arrange an account review and password reset.

4.2. Clear Desk and Screen Rules

- Be aware of your surroundings, especially when travelling, and ensure that no unauthorized individuals can see sensitive information or overhear confidential conversations.
- Do lock all mobile and desktop devices when unoccupied.
- Don't change any session time-outs and lockouts that have been implemented on systems.
- Do take care of screens so that unauthorized people cannot easily see the information displayed.
- Do remain aware of situations where unauthorized people, including visitors, may overlook your screens.
- When permitted to working from home, always keep a clear desk, store work papers in locked rooms or filing cabinets and ensure people who share your living space can't view your screen, have no access to your systems and can't overhear your work conversations.

4.3. Physical Access and Security

The following instructions apply to Users (including employees, contractors and third-party service providers who have access to our systems and information) and people given access to Lifezone offices or work areas.

- Do review and understand any instructions given if you are granted access to any secure area that is not your usual place of work.
- Do inform security or reception of visitors that you are expecting well in advance.
- Always escort your visitors and assign them specific work areas for the time of their visits, especially if people work for extended periods within Lifezone offices and work areas (auditors, investment bankers, technical and business consultants, tax advisors, etc.)
- Keep secure doors closed and never allow anyone to tailgate behind you through a secure entry point.
- Don't lend anyone your ID badge or expose it to possible theft or loss.
- Do challenge and report anyone whom you are not made aware of, who is not a known colleague and who is not wearing an ID badge.
- Remain vigilant whilst in offices, work areas and secure areas.
- Don't tell anyone a door access PIN code or don't write your PIN code down.
- Do check vacant areas for signs of unauthorized access.
- Do not use photographic, video or audio recording equipment within the Lifezone offices and work areas unless with prior permission from senior management (board of C-level executives).
- Don't leave confidential or classified information unattended, or in clear view of visitors. This includes information on your screen or device.
- Restrict access to secure IT areas using keys, badge systems and biometric authentication.
- Install environmental protection systems such as fire suppression heat systems and temperature monitoring in server rooms and data centers.
- Always ensure that doors and windows are secure before leaving if you are the last one out of the area.

4.4. General Use and Ownership

- Do promptly report theft, loss, or unauthorized disclosure of Lifezone corporate information, data or access to information assets.
- Lifezone is a publicly listed company, therefore never disclose material non-public information to external parties, if not required by law, regulations or strictly necessary to do your job duties. If it is necessary to share or disclose material non-public information with third-parties to conduct business consult a member of the Lifezone Disclosure Committee or the Legal Department (legal@lifezonemetals.com) in case in doubt **before** disclosing any information.
- Do access, use or share Lifezone proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.
- Limit and do exercise good judgment regarding the reasonableness of personal use of company equipment.
- Do consult your manager or the Chief Financial Officer if you are unclear of any policy or guideline that is in place with regards to information security and the use of information systems and assets, including mobile equipment.

- Do be aware that, for security and network maintenance purposes, authorized individuals within Lifezone may monitor equipment, systems, and network traffic at any time.

4.5. Security and Proprietary Information

- Do report anything suspicious (suspect emails, odd system behavior or accidental leaks) to itsupport@lifezonemetals.com.
- Do use system level and user level passwords that comply with the Password Policy (see the Access Control Policy).
- Don't provide access to another individual, either deliberately or through failure to secure your access.
- When participating in public forums, you should always conduct yourself in a manner that reflects positively on Lifezone.
- You should never disclose any confidential or proprietary information about Lifezone, its clients, or its operations.
- Any opinion expressed should include a disclaimer that it is a personal opinion and not that of Lifezone.
- Do use extreme caution when opening email attachments received from unknown senders or included in unexpectedly received communication, even from a known individual or company, as these may contain malware.

4.6. Unacceptable Use

The following activities are, in general, prohibited.

Employees, consultants and contractors may be exempted from these restrictions during their legitimate job responsibilities (e.g. IT management and systems administration staff may need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee, consultant or contractor of Lifezone authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Lifezone-owned resources.

The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.7. System and Network Activities

- Don't violate anyone's intellectual property or copyright or copy or distribute any material protected by copyright without the owner's / author's consent.
- Don't 'install or distribute unlicensed (pirated) software without a valid license.
- Don't access data, servers, or accounts for anything unrelated to Lifezone business.
- Do not attempt to access systems for which you do not have any permission
- Don't export software or technical information without ensuring compliance with export control laws and consult IT management first. A rule especially relevant for exploration and mining data.
- Don't introduce malicious software (viruses, worms, trojans, ransomware, etc.) into any network or server.
- Don't share your account credentials or let anyone else use your account.

- Don’t use Lifezone systems to access or distribute material that violates sexual harassment or hostile workplace laws or regulations.
- Don’t make fraudulent offers for products or services through any Lifezone account.
- Don’t make any warranty statements unless it’s within your official job responsibilities.
- Don’t cause security breaches or disrupt network communications (e.g. unauthorized data access, denial of service, packet spoofing).
- Don’t perform port or security scans without prior approval.
- Don’t intercept or monitor data unless it’s part of your regular job duties.
- Don’t bypass or tamper with security measures on any host, network, or account.
- Don’t set up honeypots, honeynets, or similar technology on Lifezone’s network.
- Don’t share lists of or information about Lifezone employees with anyone outside Lifezone.

4.8. Email and Communication Activities

- Don’t send unsolicited emails or spam.
- Don’t harass anyone through email, phone, text, or other communication methods.
- Don’t change, forge or misuse email header information without proper authorization.
- Don’t create or forward chain letters, Ponzi, or pyramid schemes.
- Don’t send unsolicited emails on behalf of or to promote any Lifezone service.
- Do be aware that when using company resources to access and use the internet, you are representing the company.
- Do use e-mail communication for business purposes and within your job duties.

4.9. Blogging and Social Media

- Don’t use social media or blog during work hours and refrain from using social media disrupting your work duties.
- Don’t reveal Lifezone’s confidential or proprietary information (including trade secrets) in blogs or social media posts.
- Don’t post content that damages Lifezone’s reputation or includes discrimination, defamation, or harassment.
- Don’t present personal opinions as Lifezone’s official stance or imply you speak for Lifezone.
- Don’t use Lifezone trademarks, logos, or intellectual property in blogs or social media without proper authorization and in non-business context.
- Do clearly indicate that "the opinions expressed are my own and not necessarily those of the company", wherever you state an affiliation to Lifezone and its group companies.
- Do blog or post professionally and responsibly, complying with this policy, protecting Lifezone’s interests.

5. Policy Review and Compliance

This policy will be reviewed at least annually and updated after significant changes in regulations or organizational structure.

IT management will verify compliance with this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Any exception to the policy must be approved by IT management in advance.

A User (employee or contractor) found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Policies and Definitions

Lifezone ensures that security policies, standards and procedures are readily available to all Users (including employees, contractors and third-party service providers who have access to our systems and information).

The current policies can be accessed on Lifezone's SharePoint folder "Policies and Procedures". Currently the following policies are available under:
https://lifezonemetalsltd.sharepoint.com.mcas.ms/sites/LifezoneMetalsIntranet/Policy%20%20Procedures/Forms/AllItems.aspx?McasTsid=20892&McasCtx=4

1. Acceptable Use Policy
2. Information Security Policy
3. Information Security Program
4. Incident Management Procedure
5. Disaster Recovery Plan

Definition and terms in this document can be found in the SANS Glossary or KnowBe4 Glossary located at:

- https://www.sans.org/security-resources/glossary-of-terms
- https://www.knowbe4.com/knowbe4-glossary