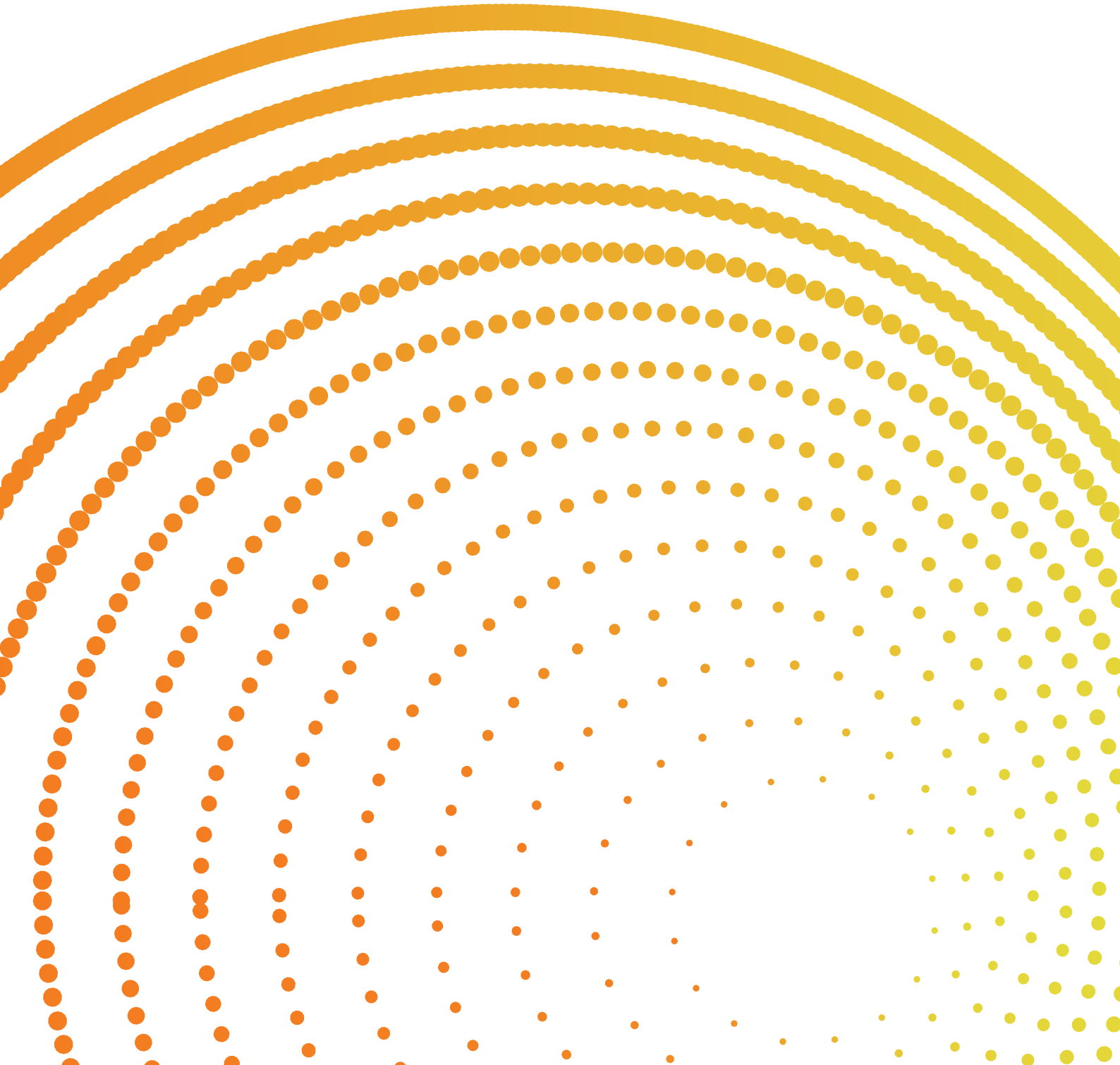
Acceptable Use of Information Systems Policy 2022

Molycop Legal



Acceptable Use of Information Systems Policy

In this Acceptable Use of Information Systems Policy **(this Policy)**, Molycop means any company or business within the Molycop group of companies and businesses, including any other companies and businesses that may be acquired by or form part of the Molycop group from time to time.

1.0 Policy Overview

This Policy sets out guidelines for acceptable use of Molycop's information systems (including, but not limited to, company-provided laptops, email accounts, instant messaging accounts, mobile devices (including phones, tablets, hotspots and related services) by any party, including employees, contractors and visitors.

Molycop provides employees with access to information systems for the primary purpose of assisting them to carry out their duties. Employees may use these systems for limited reasonable personal purposes, provided such use is consistent with this Policy.

Acceptance of this Policy is a condition of use for Molycop's information systems.

Questions or concerns relating to this Policy should be directed to your supervisor or your Molycop Human Resources contact.

Note: All references to employees in this Policy should be read to include and apply equally to contractors, visitors and all other users of Molycop's information systems.

2.0 Guiding Principles

- Molycop provides information systems for specific business purposes. The use of these systems for other purposes may present a threat to Molycop's system efficiency and security
- All electronic communications using Molycop's information systems are regarded as Molycop's records, and as such Molycop reserves the right to monitor use of its information systems and retain any related information at its discretion. This includes but is not limited to monitoring the nature and content of e-mail, instant messaging and internet usage, and restricting the transfer of certain material
- All users of Molycop's information systems should be aware of their responsibilities in relation to such access or use - particularly about the transfer or transmission of company-sensitive or inappropriate material within or external to Molycop. All employees are expected (upon commencement of employment, engagement and periodically) to provide formal acceptance of such responsibilities. Use of Molycop's information systems implies acceptance of such responsibilities
- There are significant costs incurred by the company to provide access to our information systems. Employees must use proper judgement to not incur unnecessary costs in their use
- While not intending to discourage or unduly limit individual expression or online activity outside the workplace, employees are expected to use social media in a way that does not damage the reputation or interests of Molycop or cause harm to other employees.

3.0 System Security

All information stored on or generated by or in connection with Molycop's information systems is the property of Molycop and as such must be treated as any other asset of Molycop. Every employee has a responsibility to protect Molycop information from accidental and unauthorised access, disclosure, modification or deletion.

Employees must use equipment issued by Molycop, or other companies to facilitate business with Molycop only for its intended purpose. Employees must return all such equipment to Molycop upon termination of contract or employment.

Employees are responsible for the safe keeping of all equipment that is issued or made available to them and must take reasonable steps to ensure that it is not damaged or stolen. All Molycop property must be returned in an acceptable condition upon termination of contract or employment (e.g. computers, printers, monitors, mobile devices, keys, ID cards). Employees must inform the local Molycop IT representative as soon as practical should the employee lose their device so that Molycop can remotely disable or reset the device.

Employees must not:

- disclose their password or other personal logon credentials to any other person or organisation (and must change the password or logon credential should they suspect that it is no longer secret). This includes not displaying your passwords within public view
- access, or attempt to gain access, to any Molycop data, information system, or restricted area to which they are not authorised (the nominated owners/custodians of such data or area must authorise access)
- access, or attempt to gain access, to other companies' systems without authorisation from that company
- copy, remove or divulge Molycop information (including customer lists, printed documents, or electronic data) without the authorisation of the owner/custodian
- abuse, dismantle, install or alter equipment or software without authorisation
- uninstall, change, disable, bypass or otherwise interfere with the operation of anti-virus, firewall, passcode locks (including PINs), management, protection, or monitoring systems
- install unlicensed and/or unauthorised software on Molycop devices or networks
- bypass Molycop's filtering and security systems using an unauthorised connection to the internet or other network
- install or connect malicious software or devices such as key-loggers or password-crackers to a Molycop device or network

If it is suspected that a device containing Molycop information is lost, stolen or misused then Molycop may:

- block access to the device
- wipe all information from the device; and/or
- remove or confiscate or require the employee to return or surrender the device for detailed examination.

4.0 Cyber Security Compliance

Molycop takes cyber security very seriously and every employee plays a vital component of its success. Therefore, employees must continuously practice good cyber-aware behavior including:

- Completing all requested cybersecurity training in a timely manner
- Reporting suspicious behavior and suspected cyber security breach or compromise to any Molycop IT employee immediately
- If working remotely, ensuring compliance with all facets of the "Molycop Remote Work Policy"

Note: once printed this becomes a non-controlled document

5.0 Acceptable Use

Molycop provides access to information systems for work-related activities.

Reasonable personal usage is acceptable, provided that the use is moderate in time, does not incur significant cost or inconvenience to Molycop, does not interfere with the employment duties of the employee or his/her colleagues, and does not breach any of the requirements of this Policy. "Reasonableness" is assessed in two ways.

Content: Refer to the Molycop Code of Conduct.

Business relevance: Operational/business requirements must take precedence over all other use.

Employees must not use Molycop's information systems:

- using another person's username and password
- for personal commercial purposes
- to propagate chain letters or hoaxes or send unsolicited bulk messages (spam) to internal or external recipients
- to access non-Molycop instant messaging systems for non-business purposes
- to access online movie or streaming services such as Netflix, Hulu, Stan, etc
- to harass, abuse, or defame any person
- to receive and/or transmit pornography, profanity or other offensive material
- for gambling purposes
- to play on-line or network games
- to obtain, possess, or transmit illegal or pirated material
- to obtain, possess, or transmit confidential information without authorisation
- for disseminating personal contact information of Molycop's employees, customers, suppliers, or other related parties without their consent
- for any other illegal purpose
- in a way that knowingly causes interference with or disruption to any network, information service, equipment or any user thereof
- for anything which will or may bring Molycop into disrepute
- to cause Molycop or any of its customers, suppliers or other associates to bear unreasonable risks or costs
- to cause disruption to any of Molycop's business or services or be in breach of any privacy obligations

6.0 Copyrighted or Licensed Information

Molycop uses a significant amount of information that is protected by copyright or licence. Employees must not use, copy, publish or perform any other action with such information where it breaches the licence or copyright terms.

7.0 Spam

Spam is unsolicited "junk" email sent to large numbers of people to promote products or services and may contain offensive material. Molycop is continually reviewing and improving the processes by which the emails are blocked before it reaches the employee. However, from time to time, employees may receive spam emails.

Employees who receive large amounts of spam should contact their Molycop IT representative so that preventative measures can be implemented.

8.0 Social Media (Facebook, Twitter, Tiktok, Instagram, Linkedin, etc.)

Other Than In Exceptional circumstances, where there is a clear business benefit, Molycop employees should not access social media through the Molycop network.

Users of social media sites and online forums are reminded that their participation in such sites remains subject to the Molycop Code of Conduct. Broad responsibilities under the Code of Conduct include, but are not limited to:

- not disclosing market sensitive, confidential or personal information obtained through work • not harassing, bullying or demeaning any person or company
- not implying that you represent Molycop or that your personal views are endorsed by Molycop not saying or doing anything that will bring Molycop into disrepute or undermine the effectiveness of yourself or others at work
- It is strongly recommended that employees who use social media sites take adequate precautions to ensure their own privacy and security.

9.0 Maintenance of Data and Records

Employees are responsible for storing company data in Molycop enterprise datastores (ie. One Drive, Sharepoint, D365, local file servers). Molycop data should not be stored locally on computers, external drives, etc as these devices are susceptible to failure and/or loss. Employees are responsible for the compilation and handover of Molycop's records entrusted to them upon leaving Molycop or changing roles.

Electronic files and records must not be deleted or destroyed without the approval of the employee's manager, and then only in compliance with any accepted and/or Molycop- documented standards for record retention. Users should contact their Molycop IT Representative if in need of information or assistance with respect to backing up or archiving important information.

10.0 Remote Access to Molycop Systems

Accessing internal/non-cloud, Molycop systems remotely via VPN is only allowed from Molycop issued and managed computers. VPN access must be approved by the requestor's manager/supervisor and by the local IT leader or global IT support leader. If connecting to Molycop systems cannot be accomplished from a Molycop issued/managed computer (ie. managed service provider), approval must be obtained from the Molycop Chief Information Officer or his/her delegate(s).

11.0 Use of Personally Owned Mobile Devices

Molycop allows employees to utilize personally owned mobile devices (mobile phones, smart phones, iPad, tablets, etc.) to access specific Molycop data. This data includes email, calendars, instant messaging, cloud storage, security cameras, etc.

It is the responsibility of the individual employee (user) to:

- Ensure all data is backed up appropriately on the mobile device. Molycop will not be liable for any personal data lost on any mobile device
- Ensure the operating system software on the device is current
- Inform the Molycop IT Team as soon as practical should the employee lose their device so that Molycop IT can remotely remove company data.

Application distribution platforms (i.e., iTunes, Google Play, etc.) are the responsibility of the employee and must not be linked to Molycop corporate credit card accounts.

Access is subject to the following conditions:

- All costs associated with the device are at the employee's expense unless approved by the employee's Regional President or a Molycop Corporate Head Office executive
- Molycop IT will not provide support or assistance in the setup or troubleshooting of the device should it not work properly
- The employee must permit Molycop to install a mobile device management tool and/or other similar software on the device to provide appropriate monitoring and security
- If the employee's employment or engagement with Molycop ends for any reason, the employee must assist in the deletion of all Molycop data immediately from all their personally owned devices and, if requested by Molycop IT, temporarily hand over such devices to the local Molycop IT representative to screen the devices and wipe any remaining Molycop data from them

Except with the written approval of their Regional President, employees must not install a Molycop SIM into their own personal device. The use of a Molycop SIM in a personally owned device may be approved only under exceptional circumstances, where use of a Molycop provided mobile phone or smart phone is impractical or undesirable.

12.0 Privacy

Molycop will comply with relevant privacy legislation and principles with respect to the recording and monitoring of systems use. Databases and other records are subject to Molycop's Privacy Policy and the related privacy principles.

However, given the nature of such communications, Molycop cannot guarantee the privacy of electronic communications - particularly when those communications leave the Molycop network. Although these communications or other information may be deleted by the user, copies of them may be retained in backups or archives for an indefinite period.

Access rights to files, mailboxes, logs and other similar information is normally restricted to the Molycop IT staff with responsibility for administering those systems, and while such information may generally be considered private, it may be disclosed to other parties where there is a legitimate reason or legal requirement.

13.0 General Disclaimer on Emails Addressed to External Recipients

Users should be aware that all emails addressed to recipients outside the Molycop network are automatically tagged by Molycop's email provider with the following disclaimer or similar, as may be modified from time to time:

The material contained in this email is confidential and may be subject to legal professional privilege and/or copyright. Please do not re-transmit, distribute, copy or commercialise any of the material in this message unless you are authorised to do so. If you are not the intended recipient, use, disclosure or copying of this information is prohibited. If you have received this document in error, please advise the sender and delete the document. None of Molycop, its related bodies corporate or the sender accept responsibility for any viruses contained in this email or any attachments. All and any rights as to confidentiality, legal professional privilege and copyright are expressly reserved.

14.0 Consequences of Unacceptable Use

Molycop will review alleged breaches of this Policy on an individual basis, in accordance with ordinary disciplinary processes. Serious breaches may result in dismissal or the withdrawal of access to specific information systems.

15.0 User Agreement

Upon an employee's first access of any Molycop information system, the employee is deemed to have agreed to all items outlined in this Policy and agrees to comply with all the requirements set out in the policy.

Jim Anderson
Chief Executive Officer
August 2023

Note: once printed this becomes a non-controlled document

MOLYCOP

molycop.com