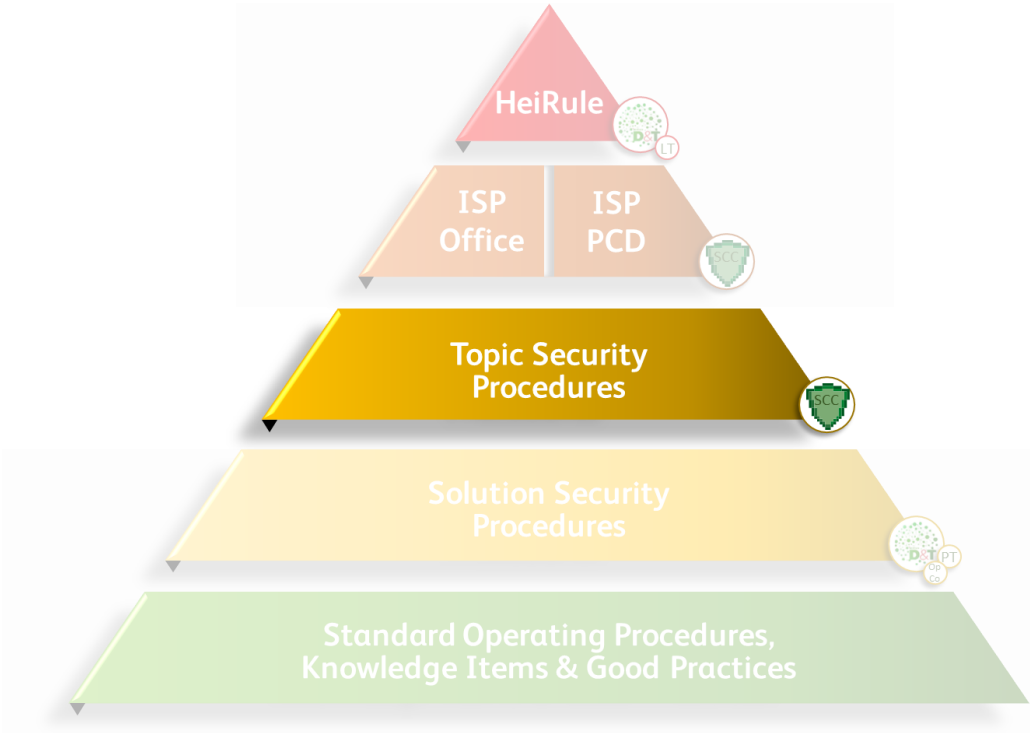
HEINEKEN Systems Global Acceptable Use Policy

[ID.GV-1] [Governance]



Executive Summary

Information is a vital corporate asset of HEINEKEN and requires protection from unauthorized access, modification, disclosure or destruction. Use of any internal or external system for inappropriate personal interest and any other purpose that may be in violation of laws, the HEIRules or other HEINEKEN business interests is prohibited. This Policy contains guidance in respect of the daily usage of HEINEKEN information assets and systems in order to ensure business continuity and prevent any operational, legal and reputational risks. This Policy is part of the Information Security Policy House of HEINEKEN.

Summary of changes compared to current version

The document has been renewed in line with the current Information Security Policy (ISP) here and all the guidelines and procedures mentioned and linked in all this document

Functional Owner of this Topic Security Procedure

Name	Function
Security Governance	Owner of the Security Policy House

Effective date of current version/ Transition period

Effective date	02.05.2024
End of transition period	02.11.2024

Applicable for

Applicable for	See Chapter 1

Approval by the Owner and higher body if needed

Approving body	Date
Global Information Security	28/11/2023
Global Design Authority – Technology Products	04/12/2023

Next planned review

Review	Date/ Trigger
Next review date planned	02.05.2026
Based on trigger	Biyearly review cycle with SMEs.

Expert group members (SME) for document creation/review/approval – SMEs

Name of SME	Function
Tonne Mulder	D&T Manager Global Information Security
Massimo Berti	Global D&T Privacy Officer
Hendrik Jan Bolte	Senior Legal Counsel D&T
Ricardo Schluter	Global architecture & innovation
Pieter Siedsma	Global DA & TP

Table of Contents

0 Document scope

This Policy aims to safeguard HEINEKEN Systems *(see annex for definition)*.
Use of any internal or external system for inappropriate personal interest and any other purpose that may be in violation of laws, the HEIRules or other HEINEKEN business interests is prohibited. This Policy contains guidance in respect of the daily usage of HEINEKEN Systems to ensure business continuity and prevent any operational, legal and reputational risks. Capitalized terms in this Policy have the meaning set out in Annex 1 Terms and Definitions.

1 Applicability of the Policy

Applicability of the Policy

This Policy applies to:

(i) individuals employed by any HEINEKEN entities in the Netherlands , regardless of the type of contract or the location of their work using or having access to HEINEKEN Systems,

(ii) (ii) individuals working for HEINEKEN entities in the Netherlands through a third party contract using or having access to HEINEKEN Systems and

(iii) (iii) third party service providers contracted by HEINEKEN entities in the Netherlands using or having access to HEINEKEN Systems.

Each User has the obligation and responsibility to ensure that they are familiar with the contents of and comply with this Policy.

This Policy is available in the Information Security Policy House here and is made available e.g. when onboarding employees.

Mandatory (local) HEINEKEN Systems Acceptable Use Policy

It is mandatory for all OpCo's to have a policy regarding acceptable use of HEINEKEN Systems and possible monitoring in this respect. OpCos can use or refer to this Policy as a template and where necessary tailor it, considering the HEINEKEN Privacy Procedures and applicable local law.

2 Monitoring and enforcement

To ensure the continuity of HEINEKEN's business processes and to prevent inappropriate usage of HEINEKEN Systems, the usage of HEINEKEN systems may be monitored, logged and registered as further set out in section 11 of this Policy. Monitoring, logging and registering of HEINEKEN Systems by HEINEKEN shall only take place in accordance with the HEINEKEN Privacy Procedures and applicable local law.

Users who do not comply with this Policy and/or attempt to disable, defeat, or circumvent any security mechanism may be subject to disciplinary actions.

If a User acts in contravention of this Policy, the interests of the company and/or the generally accepted standards and principles for the use of HEINEKEN Systems, he/she may incur in actions that can range from a verbal reprimand to dismissal.

For more details, please refer to the Policy on disciplinary measures here

3 Relation to other HEINEKEN Policies

This Policy is part of the Information Security Policy House of HEINEKEN. This Policy is related to, and in some respects a specification of (parts of) other HEINEKEN policies. Please consult the HEINEKEN Code of Business Conduct, the Privacy Procedures, the Information Security Procedure and the HEINEKEN Fraud Policy/Fraud Response Protocol.

These Policies are part of the *HEINEKEN Company Rulebook* and can be found on http://heiport.heiway.net *(COMPANY section)*

4 General statements

Main do's and don'ts

4.1. Users shall not use HEINEKEN Systems to:

- engage in activity that is illegal under applicable law or in conflict with the HeiRules or HEINEKEN Policies;
- engage in any activities that may cause embarrassment, loss of reputation, or other harm to HEINEKEN;
- disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, insulting, threatening, obscene or otherwise inappropriate messages or media;
- engage in activities that cause an invasion of privacy;
- engage in activities that cause disruption to the workplace environment or create a hostile workplace;
- make fraudulent offers for products or services.

In addition, Users shall not:

- forge messages, use another employee's e-mail or other HEINEKEN information system account, or attempt to disguise their identity including the use of unauthorized IP masking, proxy servers, encryption or VPN software while connected to an HEINEKEN network or while using HEINEKEN System;
- reveal HEINEKEN network and systems passwords to others, including family, friends, or other members of the household;
- install, disconnect, modify, and/or relocate equipment, without the express authority of the HEINEKEN Digital & Technology department;
- connect or install wireless connection devices and wireless access points (wireless hubs/routers) or allowing the "wired" connection of the HEINEKEN corporate network to an unauthorized non-HEINEKEN local or wide area network.

4.2. Users are prohibited from accessing or attempting to access the accounts or credentials of others, breaching or attempting to breach security measures of HEINEKEN or another company's computer software, hardware, network communications and/or telecommunications systems, except with the express permission of the company owning the system being accessed or within the scope of regular documented duties. This includes, but is not limited to:

- any attempts at port scanning or security scanning without the prior written permission from the HEINEKEN Information Security team;
- any attempts at network monitoring which will intercept data not intended for the employee's computer, unless this activity is a part of the Users normal job function;
- any attempts at circumventing User authentication or security of any computer, network or account;
- any use of unauthorized remote-control software.

4.3. HEINEKEN file storage systems are designed for production needs of Users.
Any information that is not HEINEKEN related shall not be stored on HEINEKEN file servers. Within reason, data for personal use may be incidentally kept on local computer drives but should be clearly marked as personal *(e.g. by including "PRIVATE" in the name of a file or subject of an e-mail)*.
Data for personal use may not be backed up by HEINEKEN backup and recovery systems.

4.4. Users should consult the *Topic Security Procedure for Information Classification,* available on the *Security Policy House* *here* and is made available e.g. w_to ensure proper permission is obtained before using or forwarding any HEINEKEN information.

4.5. Information of a sensitive or otherwise proprietary nature must not be shared outside of HEINEKEN via means (including but not limited to e-mail, social media, filesharing solutions) unless explicitly approved.

4.6. Devices not provided by HEINEKEN and used to access HEINEKEN information (where it's allowed by local OpCos) need to be compliant with HEINEKEN policies regarding information security. *(*refer to the local *Bring your own device policy* if and where it is allowed by the OpCo*).* HEINEKEN can block, restrict or regulate the access to HEINEKEN information with these devices without prior notice. HEINEKEN can ask the owner of these devices to allow the installation of dedicated software in order to properly protect that access to HEINEKEN information. Refusal of this request may result in denying access to HEINEKEN information resources on these specific devices.

4.7. Users shall protect the HEINEKEN Systems and the information stored and processed by following HEINEKEN information security policies and any guideline issued by the HEINEKEN Digital & Technology function.
This is valid whether you work in the office and/or on sites where the HEINEKEN network is active or whether you work remotely (smartworking, hybrid working, etc.) therefore using domestic networks and locations

Incidental personal use

4.8. Personal communications at work or via HEINEKEN Systems are subject to the same standards as any business communication. Users may use HEINEKEN Systems for incidental personal use. "Incidental" is subject to the context of how and when Users are using HEINEKEN Systems, but it can generally be defined as infrequent, unsystematic and not disruptive to work.

4.9. Incidental personal use does not include any use of HEINEKEN Systems for a business other than HEINEKEN, or any use that would violate any other HEINEKEN policy. This includes policies regarding conflicts of interest, confidentiality of information, or harassment of or discrimination against employees and third parties.

4.10. Incidental personal use does not include any use that puts a burden on HEINEKEN Systems. For instance, personal use of online video or audio streams is a drain on network resources and may interfere with business uses. Users must not install software for personal use.

4.11. If Users want to keep personal information private, HEINEKEN information assets are not advised to be used and if so, clearly mark your personal information as private. It is recommended to that Users use their own personal equipment and services are for personal information and personal use.

4.12. Users are in general responsible for exercising good judgment regarding the reasonableness of personal use.

5 Username and password

Users must comply with the following rules concerning the usage of Username and password:

- the Username and password are associated with an individual person.
- the use of generic (non-personal) accounts is not allowed unless approved by HEINEKEN Information Security.
- Users must lock the screen or log off when their device is unattended.
- A secret, unique and long password is a strong password.
- **Secret – Protect your password**
  - Keep your password to yourself, it is a personal secret.
  - Memorise your password, do not write your personal secret down anywhere.
  - If you must remember many passwords, you can use a HEINEKEN approved tool to store them in a safe way.
  - Be careful about anyone looking over your shoulder while you are entering your password.
  - Change your password immediately when you have any suspicion or indication that it could be compromised.
- **Unique – Create unique passwords for every account**

- Use different passwords for different accounts, so a unique account has a unique password.
- Re-using passwords across work and home accounts creates risks, because if one account is breached the others can be easily breached as well.

- **Long – Create a good "strong" password**
  - Create passwords of at least 12 characters.
  - Avoid personal information, such as your account name/ Username, pets, date of birth, etc. in any form (as-is, reversed, capitalised, doubled).
  - Avoid HEINEKEN brand names.
- **Easy to remember, but hard to guess**
  - String together multiple random words or a passphrase and optionally add punctuation, capitalization, numbers and special characters.
    For example: shoe type, dinner from last night, item in your room: RunnersPadthaiDesk20

- Multi Factor Authentication (MFA) is mandatory for solutions/applications accessible from external networks authenticating over Azure Active Directory *(when using your HEINEKEN credentials).*

For more details refer to the Topic Security Procedure (TSP) for password stored in the Security Policy House, *here*

6 Publishing (including social media)

- Publishing by Users, whether using HEINEKEN Systems or property, is also subject to the terms and restrictions set forth in this Policy.
- Publishing includes any form of information uploading/sharing towards non-HEINEKEN services.
  This includes, but is not limited to: social media, internet forums, translation engines, generative AI platforms (e.g. ChatGPT, DALL·E, Bard), document converters or fileshare services *(on AI topic, please refer to Joint guidance on the use of non-contracted Generative AI by employees here and here)*
- Limited and occasional use of HEINEKEN Systems to engage in publishing is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate laws or HEINEKEN policies, is not detrimental to HEINEKEN best interests, and does not interfere with User's regular work duties.
- Publishing with the use of HEINEKEN Systems is also subject to logging and monitoring *(please refer to section 11)*
- The HEINEKEN Confidential Information policy also applies to publishing. As such, Users are prohibited from revealing any HEINEKEN confidential or proprietary information, trade secrets or any other material covered by HEINEKEN Confidential Information policy when engaged in publishing *(please refer to HEINEKEN Confidential Information policy here)*

- When information may be sent as explained above, Users should use the available means of information security when sending approved confidential data and sensitive business information to an e-mail address outside the organisation *(e.g. password, encryption)*.
- Users shall not engage in any publishing/sending/forwarding that may harm or tarnish the image, reputation and/or goodwill of HEINEKEN and/or any of its employees. Users are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when publishing or otherwise engaging in any conduct prohibited by *HEINEKEN Non-Discrimination and Anti-Harassment policy (please refer to the related Business Code of Conduct here)*.
- Generating incoming private messages because of participating in non-business-related social media groups, subscribing to e-zines, electronic newsletters or the like is forbidden.
- Users may also not attribute personal statements, opinions or beliefs to HEINEKEN when engaged in publishing. If a User is expressing his or her beliefs and/or opinions in blogs/email/social media, the User may not, expressly or implicitly, represent themselves as an employee or representative of HEINEKEN. Users assume any and all risk associated with publishing.
- if Users are offered information of business/confidential/sensitivity nature when they have not requested such, they must inform their immediate superior and the HEINEKEN Digital & Technology department.
- Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, HEINEKEN trademarks, logos and any other company intellectual property may also not be used in connection with any publishing activity.
- Any suspicious messages must be reported through the SPAM button available in Outlook *(please, refer to the phishing reporting guidelines here)* or as follows:
    - Call the **CDO number** – available 24/7 HEINEKEN wide service: **+31205239991**
    - Email to **security.incident@heineken.com** – available from **8AM-5PM CET** on a workday assistant
    - Report the information security incident via **CDO App** on your phone / Go to the **ServiceNow home page** and report a information security incident / Chat with the ServiceNow **virtual assistant**

7 Provision of Internet

HEINEKEN applies the following guidelines for security and risk management of its data and business purposes in connection with the use of Internet by Users:

- HEINEKEN may grant the right to use (a part of) the Internet, but may also withdraw such right at all times, without stating the reasons for doing so.
- HEINEKEN reserves the right to restrict, block or ban access to certain Internet sites.

8 Usage of mobile computing and storage devices

- Only mobile computing devices (i.e mobile phones, laptops, etc.) issued or otherwise checked for security by HEINEKEN may be used to access HEINEKEN Systems.
- Confidential data and sensitive business information must be protected when stored on a mobile computing or storage device and brought outside the organization (e.g. by encryption).
- Unattended mobile computing and storage devices must be physically secured: locked in an office, locked in a desk drawer or filing cabinet, or locked to a desk or cabinet via a cable lock system. In particular, these devices must not be left in parked vehicles.
- To protect confidential data and sensitive business information, Users must adhere to the controls as offered by HEINEKEN and not by-pass security controls (e.g. accepting invalid certificates, approved unexpected MFA requests).
- Users working in public spaces are required to take measures to prevent overlooking or eavesdropping by unauthorized persons in order to protect confidential and sensitive business information.
- In case confidential or sensitive business data is lost *(e.g. loss of USB stick or laptop)*, disregarding by what cause, Users are obliged to report this immediately following the channels described above.
- in case of loss of a HEINEKEN-owned mobile computing device, Users are obliged to report this using the same contacts and process described at the end of the Section 6.

9 Malware

Users must comply with the following rules concerning the prevention of malware (e.g. viruses):

- the deliberate introduction of malicious programs into the HEINEKEN Systems is strictly forbidden;
- Users are not allowed to remove or de-activate virus scanning software or interrupt scans;
- Users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware, e.g. viruses;
- the use of portable storage devices e.g. USB sticks, external hard disks increases the risk of viruses. Portable storage devices *(demonstration/ presentation copies and software updates, but also portable storage devices brought from home)* offered to Users via the post or other external logistical channels may be infected with a virus. Users must, therefore, ensure that all portable storage devices do not contain viruses prior to using them on HEINEKEN systems, or arrange a check to be done by the HEINEKEN IT department.
- Users must inform the responsible HEINEKEN IT department immediately when a virus infection could not be automatically removed by the anti-virus software.

- Users must report any suspicious activity or a potential or real malware infection through the same contacts and process described at the end of the Section 6.

10 Computer and software licenses

- The downloading and installing of software and applications that are not appropriately licensed or approved for use on HEINEKEN Systems is not permitted.
- Software licensed by HEINEKEN may only be (partly or entirely) used on a single computer at any one time and may not be lent out or transferred.
- Software licensed by HEINEKEN may not be copied or changed, whether it be for internal or external use, unless it is required to install the software onto the computer for the first time.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which HEINEKEN or the User does not have an active license is strictly prohibited.

11 Monitoring, logging and registration of the usage of HEINEKEN Systems

Electronic communications or information created and stored on HEINEKEN Systems or disclosed via the HEINEKEN Systems and use of the HEINEKEN Systems may be monitored, logged and registered for safety, security, compliance and integrity purposes in accordance with the *HEINEKEN Privacy Procedures* *here* and applicable local law.
Please also refer to applicable HEINEKEN privacy notices for further information on e.g. your rights.
Monitoring, logging and registering can, for example, be used by HEINEKEN to detect and prevent system attacks via viruses and other harmful methods, to protect HEINEKEN and employee assets, to authenticate User status and access rights and identity management, to monitor compliance with applicable laws, to monitor compliance with the rules in this Policy or other HEINEKEN HeiRules and Policies and to manage operational efficiency and effectiveness, only limited to system functioning and not to individual employee functioning.

Monitoring, logging and registering shall take place via automated means *(e.g. via content filtering and limited to electronic communications data)*, unless there are specific and legitimate reasons for HEINEKEN to review content of files or emails of a User. This may include investigations requested by other enabling functions such as HR, Compliance, Legal or Audit as referred to in section 12.

Monitoring, logging and registering (including data tracing and analysis) is conducted using information security monitoring tools. These tools are assessed for information security and privacy implications prior to their use. Monitoring is conducted by ad hoc team (part of the Cyber Defense and Operation department – CDO) that is skilled to handle tools explained above.

Administrators sign a specific document to operate how it's requested in their sphere of competences (*please, refer also to the CDO Code of Cyber security Conduct here*

Monitoring, logging and registration may be carried out at random, or targeted as part of an investigation into non-compliance by a particular User with the HEINEKEN Code of Business Conduct and its underlying polices and/or applicable laws (see section 12 below), or if the account of the User might be compromised.

12 Investigation - process

Prohibited or improper use of HEINEKEN Systems is not acceptable or permitted.
Maintaining the security, confidentiality, integrity, and availability of information stored in HEINEKEN Systems is a responsibility of all Users.

As part of an investigation into non-compliance by a particular User with the HEINEKEN Code of Business Conduct, its underlying polices and/or applicable laws, a review may be conducted of the use and contents of the HEINEKEN Systems used by the relevant User.
Such investigative action is subject to certain conditions, notably compliance with data privacy laws, and pre-approval from the HEINEKEN Global Integrity Committee. A relevant member of the Speak Up Global Review Team may liaise directly with T-systems on the collection of data from HEINEKEN Systems used by the relevant User.

For more details, please refer to the:
- *Business Code of Conduct here*
- *Speak Up investigation guide here*

13 Governance

Compliance checking

Compliance with this Policy as applicable further to section 1 of this Policy is checked through Information Risk Self-assessment and IT audits.
This audit may be conducted by Global Audit or ad hoc external audit by request.
Local audits in the OpCos may be requested to verify ad hoc behaviours explained in the Sections from 1 to 10.

Derogations from this Policy, updates of this Policy and local policies

In case a derogation from this Policy is required in the Netherlands, the standard derogation process needs to be followed *(refer to the standard derogation process here).*

Updates of this Policy in the Netherlands needs to be reviewed and approved by:
- the Global Design Authority – Technology Products (DA-TP)
- the Global Digital Tech ology and Privacy Office function (GDT&PO)

For help in respect of local policies regarding acceptable use of HEINEKEN Systems and possible monitoring hereof, please contact Global Security Governance department or your local Privacy/Security Officer.

Annex 1 – TERMS AND DEFINITIONS

Term	Definition
Asset	Any tangible of intangible object that belongs to HEINEKEN and has any value (monetary or otherwise).
Availability	The property of being accessible and usable upon demand by an authorized entity.
Confidential information	It's defined as information that belongs to the HEINEKEN organization or a person that should not be made public. It represents any sensitive business information and/or basic personal data.
Confidentiality	The property that information is not made available or disclosed to unauthorised individuals, entities, or processes.
HEINEKEN	Each company that is majority owned and controlled, directly or indirectly, by Heineken N.V.
HEINEKEN Systems	IT assets & information systems owned or operated by or on behalf of HEINEKEN, whether located on HEINEKEN premises or at an off-site location or hosted by a third party, such as networks, desktop computers, laptop computers/notebooks, mobile (storage) devices , use of e-mail/ notes, intranet/ Internet and phones, mobile phones and voicemail, multifunctional printers, information systems and software and solutions (including shareware).
HEINEKEN Privacy Procedures	Global privacy policies of HEINEKEN setting out standards on how HEINEKEN processes personal data of employees, consumers, suppliers and business partners.
Information security	The preservation of confidentiality, integrity, and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.
Integrity	The property of safeguarding the accuracy and completeness of assets.
Malware	Short for ***mal****icious soft****ware***, software designed specifically to damage or disrupt a system, such as a *virus* or a *Trojan horse*
MFA (Multi Factor Authentication)	MFA (Multi Factor Authentication) an authentication method that requires a User to provide at least two verification factors (not only a single password) in order to access a website, application, resource, system.
Password	Passwords are the key to secure access information and business applications and ensure the integrity and confidentiality of HEINEKEN data.

Policy	A policy is a statement of intent and is implemented as a procedure or protocol
Sensitive information	It is business information that should be shared only with a very limited group of employees and should be treated with the utmost care. Represents very sensitive business and personal data with the highest possible levels of confidentiality, integrity, and restricted availability.
User	(i) an individual employed by any HEINEKEN company, regardless of the type of contract or the location of their work using or having access to HEINEKEN Systems; or (ii) anindivdual working for HEINEKEN through a third party contract using or having access to HEINEKEN Systems; or (iii) athird party service provider using or having access to HEINEKEN Systems.
UserID	Users of Systems are represented by a unique identifier an UserID. Also called Username or User account.