Security instructions

All employees must read and sign these security instructions before starting their employment.

bouvet

Effective from:
01.11.2024

Version:
3.1

Version history

Versjon	Dato	Beskrivelse	Ansvarlig
2.0	01.08.2023	Baseline	Knut Dischington
3.0	20.01.2024	Minor adjustments to chapter 7 and 9, updated signature fields	Knut Dischington
3.01	01.02.2024	Chapter 16, added «Uppercase»	Knut Dischington
3.1	01.11.2024	New chapter 4	Knut Dischington

1. General information about personal responsibility and IT security

No information may be disclosed to any external parties concerning login procedures, usernames and/or shared passwords for the various systems that form part of Bouvet's or Bouvet's customers' infrastructure.

This also applies after employees leave the company.

All personal passwords must be kept strictly private. You must ensure that your passwords cannot be easily guessed. You must not share your passwords with colleagues, family members, cohabitants or any other third parties.

You must not write passwords down so that others can access them, and you must not switch on automatic password saving on browsers.

Two-factor authentication must be used for logins whenever possible.

If you suspect that someone knows your password, you must have your password changed immediately and it must be reported as a security incident.

Each employee undertakes to stay up to date with and follow the rules for information security and basic security competence for their roles, as described on Bouvet's intranet.

2. Email and calendar

The email system is intended to be a work tool. Personal use of email is permitted, provided this does not interfere with work duties. Be careful about what you use Bouvet email for.

The calendar in the email system can be read by all colleagues. Therefore, avoid entering any sensitive information or mark it "private".

3. The company's right to access

While the company does not routinely monitor the content of employees' email or other communications or storage media, the company reserves the right to access if:

- this is necessary to perform daily operations (e.g. in connection with illness or other absence)
- this is necessary to safeguard the company's legitimate interests
- there is a justified suspicion of a serious breach of duty or other circumstances that may provide grounds for termination or dismissal

The decision on access is made by the Personnel Manager, together with the Chief Information Security Officer (CISO). The employee will, as far as possible, be notified in advance if access is required and be given the opportunity to make a statement before the inspection is carried out. The employee must, as far as possible, be given the opportunity to be present during the inspection, and is entitled to be assisted by a union or other representative. How the inspection was carried out, what was inspected and who participated must be documented in writing.

4. Use of Bouvet ID Card

All employees must, while present in our premises, always wear their Bouvet ID card with photo and name (access card) visibly around their neck. This is to effectively identify any non-employees present in the premises and enable taking necessary actions.

You shall not wear the access card visibly outside our premises.

You shall not publish pictures showing your access card on the internet, including all forms of online communities, social media, and other types of channels, without prior approval from the CISO.

Remember, similar rules may apply at the customer's site, so obtain permission first.

5. Logging and protection against undesired incidents

Bouvet uses various tools to protect computers, identities and other infrastructure against cyberattacks and undesired incidents. These tools analyse traffic and content on Bouvet's computers and other Bouvet-controlled devices. When notified by these tools, Internal IT & Security will analyse the specific case and notify the user if any action needs to be taken. A "Security Incident Report" will always be created in Bouvet's incident system and copied to the HR Manager.

6. Storage

All material, such as documents, source code, designs, data etc., that is created by the employee on behalf of Bouvet or Bouvet's customers must be stored on Bouvet-administered or customer-administered IT solutions. Such material must not be stored on third-party solutions where Bouvet and/or the customer do not have administrative control over access and content, for example Dropbox, Apple iCloud or Google Drive.

7. Work tools

All employees will be assigned the necessary work tools when starting employment, normally a Bouvet-controlled PC or Mac and a mobile phone.

You must never lend this equipment or share it with others, whether Bouvet employees, family members or anyone else.

In connection with assignments, the employee may also receive a customer-controlled PC/Mac for use with the customer's systems and infrastructure.

Only these Bouvet- or customer-controlled devices may be used for the work. You must never log in to Bouvet's or the customer's systems and infrastructure from any other device. You must comply with Bouvet's prevailing remote-access policy.

8. Employee blogs and use of social media

The company encourages employees to make online posts about activities at Bouvet that may be of interest to third parties, e.g. breakfast seminars, interesting blog posts, presentations given by employees or similar.

You must exercise discretion with regard to what you say online about Bouvet, customers, partners, competitors and colleagues. Remember that in practice it is difficult to distinguish between what you say as a representative of Bouvet and what you say as a private individual. Always be polite and respectful.

If illegal material is published on behalf of Bouvet or material is published that could harm the company's reputation, contact the Communications Officer for advice on how to proceed.

Signing political petitions

Naturally, it is not a matter for Bouvet if you wish to sign a political petition, but we ask you to do so as a private individual. We request that you do not sign as a representative of Bouvet.

9. Policy for the use of copyright-protected material

Bouvet purchases licences to use software from a number of companies/software developers. Bouvet does not own this software or the accompanying documentation, and, unless authorised by the software developer, is not entitled to copy this software, except for backup purposes. Bouvet's employees must use software in accordance with the licence terms for the software in question.

Bouvet's employees must not download or upload unauthorised software or other copyright-protected material such as videos, music, images etc. over the internet.

Under applicable copyright laws, illegal copying of software may result in civil lawsuits and criminal liability, including fines and imprisonment. Bouvet does not permit the copying of software or other copyright-protected material. Any Bouvet employees who store, acquire or use unauthorised copies of copyright-protected material for computers must expect to be held responsible for such actions, and could potentially be dismissed.

If you are in any doubt as to whether you can install, copy or use a particular copy of software or use a program or other copyright-protected material, you must consult the line manager before taking any further action.

Downloading, storing or disseminating criminal material such as child pornography, racist material etc. is strictly prohibited and may provide grounds for dismissal.

Ownership rights, copyrights and other intellectual property rights to the results of assignments, including the right to change, process and transfer, belong to the customer or Bouvet, depending on the contract in question. Bouvet's employees may not claim copyright to any parts of the results of the assignment or material that is included in the assignment, without prior written agreement. This applies regardless of when and in what context such material is created.

10. Press/media relations

The general duty of confidentiality also applies to handling enquiries from the press and media. All such enquiries must be referred to the Communications Officer.

As Bouvet generally considers media coverage to be profile-enhancing, managers responsible for a business, professional area or product area may make general statements without prior approval if the enquiry and the subsequent publicity are considered to be professionally oriented.

Anyone speaking to the press/media must ask to review all coverage before it is printed/published. The party in question should also ask the journalist to send a copy of the coverage to Bouvet. The employee must ensure that the company's Communications Officer is made aware of the coverage.

11. Stock exchange insider trading rules

Bouvet ASA is listed on the stock exchange. This means that all employees at all of Bouvet ASA's subsidiaries are covered by the stock exchange's insider rules relating to sensitive information. The insider trading regulations are displayed on *Min side* (My Page) and must be read by everyone.

It should also be noted that if any employee, during an assignment with a customer, gains access to sensitive information or carries out assignments that it is believed could noticeably influence Bouvet's share price, the stock exchange's insider rules may come into play. Such information would include information that a sensible investor would be likely to use as part of their basis for investment decisions.

12. Employee independence

If an employee or their related parties have significant ownership interest in companies that are in, or are about to enter into, a customer or supplier relationship with Bouvet, the CEO must be informed so that they can assess potential conflicts of interest. Significant ownership interests are defined in this context as shareholdings of more than 20 per cent. Related parties means spouse/partner/cohabitant, parents, siblings and children.

13. Handling work for competing customers

As a general rule, we consider that working for multiple companies within the same business area or industry benefits both Bouvet and our customers, as Bouvet's and the consultant's industry knowledge can positively influence the quality of an assignment.

In some cases, the nature of an assignment may necessitate measures beyond the general duty of confidentiality. This applies, for example, when formulating strategies, preparing long-term action plans and developing solutions that are not to be made public before their launch date.

Agreements on security measures beyond the general duty of confidentiality must always be recorded in writing and apply for a defined period of time. Such security measures must be approved by the CEO before being offered to a customer.

14. Duty of confidentiality

All employees have a duty to maintain confidentiality concerning all matters they become aware of through their employment, both within the company and in dealings with the company's customers or partners. This applies to both customer information and internal corporate matters at Bouvet.

The duty of confidentiality continues to apply after the end of the employment relationship. When the employment relationship ends, all information considered to be confidential must be returned.

The duty of confidentiality is absolute, subject to any statutory exemptions.

15. Breaches of security procedures

Each Bouvet employee has a duty to notify any breach of procedures for information security as soon they become aware of such. A separate channel has been established for reporting such breaches, which can be accessed via the intranet.

All reports of breaches of security procedures will be investigated and actioned if necessary. Serious breaches of security procedures may lead to termination or dismissal.

16. Bouvet's customers' guidelines and regulations

The employee must always comply with Bouvet's security guidelines and, where relevant, the customer's security guidelines. If the customer's security policy is stricter than Bouvet's, the stricter policy must be complied with.

17. Declaration

I, the undersigned confirm that I have read, understand and undertake to comply with the content of these instructions. To be signed physically or digitally.

Name (UPPERCASE)

Location/Date

Signature

One copy to be retained by the employee and one copy to be returned electronically to the HR Department for archiving.