HIWE SQS
Sourcing Quality Supporter

HIWE·IT

COMPLIANCE POLICY

Prepared by: Ivan Toth	**Date: 12.11.2024.** **Rev:**	**Approved By: Tomislav Wrana**

HIWE SQS
Sourcing Quality Supporter
CROATIA
Hiwe souqusup d.o.o.

HIWE SQS
Sourcing Quality Supporter

At HIWE, we recognise the importance of compliance in maintaining the trust of our stakeholders, protecting our reputation, and ensuring the continuity of our operations. The Compliance Policy provides a systematic approach for identifying and complying with applicable laws, regulations, and contractual obligations. This policy establishes clear guidelines and procedures to ensure that compliance risks are identified, assessed, and managed effectively. By adhering to this policy, we strive to maintain the highest standards of legal and regulatory compliance.

1. Purpose

The purpose of this Compliance Policy is to establish a structured framework for managing compliance within HIWE. This policy aims to ensure that we identify and comply with all applicable laws, regulations, and contractual obligations, and that we respect and protect intellectual property rights, records, and personally identifiable information. It provides a proactive approach to managing compliance risks and ensuring the integrity of our operations.

2. Scope

This policy applies to all activities within HIWE that are subject to legal, regulatory, or contractual obligations. It covers all employees, contractors, and stakeholders involved in these activities. The policy extends to all forms of obligations, including but not limited to, laws, regulations, contracts, intellectual property rights, record-keeping requirements, privacy requirements, and cryptographic controls.

3. Responsibility

The responsibility for implementing and maintaining this Compliance Policy lies with the designated Compliance Officer at HIWE . However, it is the responsibility of all employees to adhere to the guidelines and procedures outlined in this policy, to comply with all applicable obligations, and to report any suspected breaches of this policy.

4. Procedures

4.1. Identification of Obligations

4.1.1. We will identify and understand all legal, regulatory, and contractual obligations applicable to our activities.

4.1.2. We will maintain a register of these obligations and update it regularly to reflect any changes.

4.2. Compliance with Obligations

4.2.1. We will comply with all identified obligations in the conduct of our activities.

Prepared by: Ivan Toth	**Date: 12.11.2024.** **Rev:**	**Approved By: Tomislav Wrana**

HIWE SQS
Sourcing Quality Supporter
CROATIA
Hiwe sourquasup d.o.o.

4.2.2. We will implement controls to ensure compliance, monitor their effectiveness, and take corrective action where necessary.

4.3. Intellectual Property Rights

4.3.1. We will respect and protect all intellectual property rights in the conduct of our activities.

4.3.2. We will not use or disclose any intellectual property without the appropriate authorisation or licence.

4.4. Protection of Records and Personally Identifiable Information

4.4.1. We will protect all records and personally identifiable information in accordance with applicable privacy laws and regulations.

4.4.2. We will implement controls to ensure the confidentiality, integrity, and availability of these records and information.

4.5. Cryptographic Controls

4.5.1. We will use cryptographic controls in accordance with applicable laws, regulations, and best practices.

4.5.2. We will manage cryptographic keys securely to protect the confidentiality, integrity, and availability of encrypted information.

5. Policy Review

This Compliance Policy will be periodically reviewed to ensure its ongoing relevance, effectiveness, and alignment with emerging best practices and compliance requirements. The review process will include:

5.1. Evaluation: The Compliance Officer will evaluate the policy's effectiveness in achieving its objectives, identifying areas for improvement.

5.2. Stakeholder Feedback: Feedback from stakeholders and employees will be sought to assess the effectiveness of the policy, identify areas for improvement, and address any concerns or suggestions.

5.3. Regulatory Compliance: The policy will be reviewed to ensure ongoing compliance with relevant laws, regulations, and industry standards related to compliance.

5.4. Emerging Compliance Trends: The review will consider emerging compliance trends, technologies, and threats to adapt the policy and ensure its relevance andeffectiveness.

5.5. Policy Update: Based on the review findings, necessary updates or revisions to the Compliance Policy will be made to reflect changes in compliance needs, stakeholder expectations, or emerging best practices.

By conducting regular policy reviews, we demonstrate our commitment to continuous improvement in compliance management, adapt to evolving regulatory trends, and ensure that our practices remain effective and aligned with our business goals.

This Compliance Policy serves as a guiding principle for all employees and stakeholders, emphasizing our collective responsibility to comply with all applicable laws, regulations, and contractual obligations, respect and protect intellectual property rights, protect records and personally identifiable information, and manage cryptographic controls effectively. Through our proactive compliance management efforts, we aim to foster trust, ensure operational integrity, and protect the interests of our stakeholders.

HIWE SQS
Sourcing Quality Supporter

HIWE·IT

INFORMATION SECURITY POLICY

Prepared by: Ivan Toth	**Date: 12.11.2024.** **Rev:**	**Approved By: Tomislav Wrana**

HIWE SQS
Sourcing Quality Supporter
CROATIA
Hiwe souquasup d.o.o.

HIWE SQS
Sourcing Quality Supporter

At HIWE, we are committed to maintaining the highest standards of information security. The Information Security Policy provides a systematic approach for managing and protecting our information assets. This policy establishes clear guidelines and procedures to ensure that information security risks are identified, assessed, and managed effectively. By adhering to this policy, we strive to protect our information assets from all threats, whether internal or external, deliberate or accidental, to ensure business continuity, minimise business damage, and maximise return on investments and business opportunities.

1. Purpose

The purpose of this Information Security Policy is to establish a structured framework for managing information security within HIWE. This policy aims to ensure that our information assets are adequately protected against all threats and that confidentiality, integrity, and availability of information is maintained. It provides a proactive approach to managing information security risks and ensuring compliance with legal, contractual, and regulatory requirements.

2. Scope

This policy applies to all information assets owned by HIWE, regardless of format, location, or medium. It covers all employees, contractors, and stakeholders involved in the handling, processing, storing, communicating, and protecting of information assets. The policy extends to all forms of information, including but not limited to, spoken, printed, written, and electronic forms.

3. Responsibility

The responsibility for implementing and maintaining this Information Security Policy lies with the designated Information Security Officer at HIWE. However, it is the responsibility of all employees to adhere to the guidelines and procedures outlined in this policy, to protect information assets from unauthorized access, alteration, disclosure, or destruction, and to report any suspected information security breaches.

4. Procedures

4.1. Information Security Risk Assessment

4.1.1. An information security risk assessment will be conducted at least annually to identify potential threats to HIWE 's information assets and to evaluate the potential impact and likelihood of these threats.

4.1.2. The risk assessment will be conducted in accordance with the principles outlined in ISO 27005: Information Security Risk Management.

4.2. Information Security Controls

4.2.1. Based on the results of the risk assessment, appropriate information security controls will be selected and implemented to manage the identified risks.

4.2.2. The selection of controls will be guided by the control objectives and controls outlined in ISO 27001: Information Security Management Systems.

4.3. Information Security Awareness and Training

Prepared by: Ivan Toth Toth I.	**Date: 12.11.2024.** **Rev:**	**Approved By: Tomislav Wrana** HIWE SQS Sourcing Quality Supporter CROATIA Hiwe sourquasup d.o.o.

4.3.1. All employees will receive information security awareness training upon induction and at least annually thereafter.

4.3.2. The training will cover the importance of information security, the responsibilities of employees, and the correct procedures for handling, processing, storing, and communicating information.

5. Policy Review

This Information Security Policy will be periodically reviewed to ensure its ongoing relevance, effectiveness, and alignment with emerging best practices and information security requirements. The review process will include:

5.1. Evaluation: The Information Security Officer will evaluate the policy's effectiveness in achieving its objectives, identifying areas for improvement.

5.2. Stakeholder Feedback: Feedback from stakeholders and employees will be sought to assess the effectiveness of the policy, identify areas for improvement, and address any concerns or suggestions.

5.3. Regulatory Compliance: The policy will be reviewed to ensure ongoing compliance with relevant laws, regulations, and industry standards related to information security.

5.4. Emerging Information Security Trends: The review will consider emerging information security trends, technologies, and threats to adapt the policy and ensure its relevance and effectiveness.

5.5. Policy Update: Based on the review findings, necessary updates or revisions to the Information Security Policy will be made to reflect changes in information security needs, stakeholder expectations, or emerging best practices.

By conducting regular policy reviews, we demonstrate our commitment to continuous improvement in information security, adapt to evolving security trends, and ensure that our practices remain effective and aligned with our information security goals.

This Information Security Policy serves as a guiding principle for all employees and stakeholders, emphasizing our collective responsibility to protect information assets, manage information security risks, and ensure compliance with legal, contractual, and regulatory requirements. Through our proactive information security efforts, we aim to foster trust, ensure business continuity, and protect the interests of our stakeholders.

HIWE SQS
Sourcing Quality Supporter

HIWE·IT

INFORMATION CLASSIFICATION POLICY

Prepared by: Ivan Toth	**Date: 12.11.2024.** **Rev:**	**Approved By: Tomislav Wrana**

HIWE SQS
Sourcing Quality Supporter
CROATIA
Hiwe souqusup d.o.o.

HIWE SQS
Sourcing Quality Supporter

At HIWE, we understand the importance of classifying information based on its level of sensitivity and the impact that its disclosure could have on our operations, reputation, and legal standing. The Information Classification Policy provides a systematic approach for classifying and handling our information assets. This policy establishes clear guidelines and procedures to ensure that information is appropriately classified and that suitable controls are applied based on the classification. By adhering to this policy, we strive to protect our information assets from unauthorised access, alteration, disclosure, or destruction.

1. Purpose

The purpose of this Information Classification Policy is to establish a structured framework for classifying and handling information within HIWE. This policy aims to ensure that information is classified based on its level of sensitivity and that appropriate controls are applied to protect the confidentiality, integrity, and availability of information. It provides a proactive approach to managing information security risks and ensuring compliance with legal, contractual, and regulatory requirements.

2. Scope

This policy applies to all information assets owned by HIWE, regardless of format, location, or medium. It covers all employees, contractors, and stakeholders involved in the handling, processing, storing, communicating, and protecting of information assets. The policy extends to all forms of information, including but not limited to, spoken, printed, written, and electronic forms.

3. Responsibility

The responsibility for implementing and maintaining this Information Classification Policy lies with the designated Information Security Officer at HIWE. However, it is the responsibility of all employees to adhere to the guidelines and procedures outlined in this policy, to classify information appropriately, to handle information in accordance with its classification, and to report any suspected breaches of this policy.

4. Procedures

4.1. Information Classification

4.1.1. All information assets will be classified into one of the following categories: Public, Internal, Confidential, or Secret.

4.1.2. The classification of information will be based on its level of sensitivity and the impact that its disclosure could have on HIWE.

4.1.3. The classification of information will be reviewed at regular intervals and whenever changes occur that could affect the classification.

4.2. Handling of Information

4.2.1. Information will be handled in accordance with its classification.

4.2.2. Specific handling requirements will be defined for each classification of information.

Prepared by: Ivan Toth Toth I.	**Date: 12.11.2024.** **Rev:**	**Approved By: Tomislav Wrana**

HIWE SQS
Sourcing Quality Supporter
CROATIA
Hiwe sourquasup d.o.o.

4.2.3. All employees will be trained on the handling requirements for each classification of information.

5. Policy Review

This Information Classification Policy will be periodically reviewed to ensure its ongoing relevance, effectiveness, and alignment with emerging best practices and information classification requirements. The review process will include:

5.1. Evaluation: The Information Security Officer will evaluate the policy's effectiveness in achieving its objectives, identifying areas for improvement.

5.2. Stakeholder Feedback: Feedback from stakeholders and employees will be sought to assess the effectiveness of the policy, identify areas for improvement, and address any concerns or suggestions.

5.3. Regulatory Compliance: The policy will be reviewed to ensure ongoing compliance with relevant laws, regulations, and industry standards related to information classification.

5.4. Emerging Information Classification Trends: The review will consider emerging information classification trends, technologies, and threats to adapt the policy and ensure its relevance and effectiveness.

5.5. Policy Update: Based on the review findings, necessary updates or revisions to the Information Classification Policy will be made to reflect changes in information classification needs, stakeholder expectations, or emerging best practices.

By conducting regular policy reviews, we demonstrate our commitment to continuous improvement in information classification, adapt to evolving security trends, and ensure that our practices remain effective and aligned with our information security goals.

This Information Classification Policy serves as a guiding principle for all employees and stakeholders, emphasizing ourcollective responsibility to classify and handle information appropriately, manage information security risks, and ensure compliance with legal, contractual, and regulatory requirements. Through our proactive information classification efforts, we aim to foster trust, ensure business continuity, and protect the interests of our stakeholders.