UNITED PETFOOD

United Petfood Group Cybersecurity policy

Version 2
Approved by the board of directors: 30 08 2024

United Petfood Group Cybersecurity policy

1. Scope of application

This Group Cybersecurity policy (the “Policy”) applies to United Petfood Group BV and each and every subsidiary company of United Petfood Group BV (hereinafter ‘United Petfood’ or ‘We’).

This Policy is applicable:

- to all United Petfood employees (full-time, part-time and temporary), including managers and supervisors,
- to all third parties whenever dealing with United Petfood employees (e.g. suppliers, customers, (sub)contractors, consultants, vendors, guests).

Compliance with this Policy is mandatory, and any violations will be addressed according to disciplinary procedures. Together, we can create a secure digital environment that supports our business objectives and protects our valuable information assets.

2. Cybersecurity Mission Statement

United Petfood is dedicated to protecting the confidentiality, integrity, and availability of our information assets. We aim to defend our digital infrastructure against emerging cyber threats through proactive risk management, continuous enhancement, and cultivating a culture of security mindfulness.

3. Introduction

In today's digital age, cybersecurity is a critical component of our business operations. Cyber threats are constantly evolving, and the consequences of a breach can be severe, including financial loss, reputational damage, and legal implications. As such, our company group is committed to implementing comprehensive cybersecurity measures to safeguard our information assets and ensure the continuity of our business.

This Policy outlines our approach to cybersecurity and sets forth the best practices that all employees, contractors, and third parties must follow. By adhering to these practices, we can create a secure and resilient digital environment that supports our business objectives and maintains the trust of our stakeholders.

4. Cybersecurity Best Practices

4.1. Governance and Compliance

- Establish and maintain a robust cybersecurity governance framework.
- Ensure compliance with relevant laws, regulations, and industry standards.
- Conduct regular audits and assessments to ensure Policy adherence and effectiveness.

United Petfood recognizes the importance of governance and compliance in maintaining a secure digital environment. We are committed to establishing a strong governance framework that includes clear roles and responsibilities, regular reporting, and ongoing assessments to ensure that our cybersecurity measures are effective and aligned with our business goals.

4.2. Risk Management

- Implement a risk management program to identify, assess, and mitigate cybersecurity risks.
- Conduct regular risk assessments and vulnerability scans.
- Develop and maintain an incident response plan to address potential security breaches.

Risk management is a cornerstone of our cybersecurity strategy. By identifying and assessing potential risks, we can implement appropriate measures to mitigate them and minimize their impact on our operations. Our incident response plan ensures that we are prepared to respond swiftly and effectively to any security incidents that may occur.

4.3. Access Control

- Enforce the principle of least privilege, ensuring users have only the access necessary to perform their job functions.
- Implement strong authentication mechanisms, including multi-factor authentication (MFA).
- Regularly review and update access controls to reflect changes in roles and responsibilities.

Access control is essential to protecting our information assets. By limiting access to only those who need it and implementing strong authentication measures, we can reduce the risk of unauthorized access and potential data breaches. Regular reviews ensure that our access controls remain effective and up-to-date.

4.4. Data Protection

- Ensure the encryption of sensitive data both in transit and at rest.
- Implement data classification schemes to manage and protect data based on its sensitivity.
- Establish data loss prevention (DLP) measures to prevent unauthorized data exfiltration.

Protecting our data is a top priority. We use encryption to safeguard sensitive information and data classification schemes to ensure that data is handled appropriately based on its level of sensitivity. Data loss prevention measures help us prevent unauthorized access and leakage of our valuable information.

4.5. Network Security

- Deploy firewalls, intrusion detection/prevention systems (IDS/IPS), and other network security measures.
- Segment networks to limit the spread of potential security incidents.
- Monitor network traffic for unusual or suspicious activities.

Our network security measures are designed to protect our digital infrastructure from external and internal threats. By deploying advanced security technologies and monitoring network traffic, we can detect and respond to potential security incidents before they cause significant harm.

4.6. Endpoint Security

- Implement endpoint protection solutions, including antivirus and anti-malware software.
- Ensure timely patch management and regular updates of all systems and applications.
- Utilize device management solutions to enforce security policies on all endpoints.

Endpoints, such as computers and mobile devices, are often the target of cyber-attacks. Our endpoint security measures, including antivirus software and regular updates, help protect these devices from malicious activities. Device management solutions ensure that security policies are consistently enforced across all endpoints.

4.7. Security Awareness and Training

- Conduct regular cybersecurity awareness training for all employees.
- Promote a culture of security through continuous education and awareness programs.

- Encourage the reporting of suspicious activities and potential security incidents.

Education and awareness are key components of our cybersecurity strategy. By providing regular training and promoting a culture of security, we empower our employees to recognize and respond to potential threats. Encouraging the reporting of suspicious activities helps us detect and mitigate security incidents more effectively.

4.8. Incident Response and Recovery

- Establish a comprehensive incident response plan, including roles and responsibilities.
- Conduct regular incident response exercises to test the effectiveness of the plan.
- Maintain backup and recovery procedures to ensure business continuity in the event of a cyber incident.

A well-defined incident response plan enables us to respond quickly and effectively to security incidents. Regular exercises help us test and improve the plan, while robust backup and recovery procedures ensure that we can maintain business continuity even in the face of a significant cyber event.

4.9. Third-Party Management

- Assess the cybersecurity posture of third-party vendors and partners.
- Require third parties to adhere to our cybersecurity policies and practices.
- Include cybersecurity requirements in contracts and conduct regular reviews of third-party compliance.

Our relationships with third-party vendors and partners can introduce additional cybersecurity risks. By assessing their security posture and requiring adherence to our policies, we can mitigate these risks and ensure that our partners maintain a high level of cybersecurity.

4.10. Continuous Improvement

- Stay abreast of the latest cybersecurity trends, threats, and technologies.
- Continuously evaluate and enhance our cybersecurity measures.
- Foster a culture of innovation to adapt to the evolving cybersecurity landscape.

Cybersecurity is a dynamic field that requires ongoing vigilance and adaptation. We are committed to staying informed about the latest developments and continuously improving our security measures. By fostering a culture of innovation, we can effectively address the evolving challenges of the cybersecurity landscape.

4.11. Commitment to Excellence

United Petfood is committed to maintaining a secure and resilient digital environment. By adhering to these best practices and fostering a culture of cybersecurity awareness, we aim to protect our information assets and uphold the trust of our stakeholders.

5. Governance - Roles - Responsibilities

The General Manager is responsible for implementing and monitoring this Policy at the relevant subsidiary under its supervision. This includes ensuring that all operations/activities align with the Policy's objectives and that employees comply with its guidelines. Severe violations of the Policy should be reported to Group Management, and if necessary, to the Board of Directors.

6. General

This Policy takes effect on September 1st, 2024 and replaces all previous Group Cybersecurity policies at group level.

Where a local Cybersecurity policy is implemented at the relevant subsidiary, or local standards, law and regulations differ from this Policy, the most stringent rules shall apply.

United Petfood reserves the right to amend this Policy at any time.