Политика Управления Информацией и Связанными Активами

1. Введение

Данная политика устанавливает правила и процедуры для управления информацией и связанными активами в ТОО «Компания Э-КОМ ПРАЙМ». Ее цель - обеспечить конфиденциальность, целостность и доступность информации, а также защитить активы от различных угроз и инцидентов.

2. Область Применения

Политика распространяется на всех сотрудников, подрядчиков, партнеров и других сторон, имеющих доступ к информации и активам ТОО «Компания Э-КОМ ПРАЙМ».

3. Определения

- **Информация**: Все данные, хранящиеся в электронном или физическом виде, которые имеют ценность для организации.
- **Активы**: Оборудование, программное обеспечение, информационные системы, документы и другие ресурсы, используемые для обработки, хранения и передачи информации.

4. Роли и Ответственности

- **Руководство**: Обеспечение реализации политики и выделение необходимых ресурсов.
- **Служба ИТ и Безопасности**: Разработка и внедрение процедур защиты информации и управления активами.
- **Сотрудники**: Соблюдение установленных правил и процедур, сообщать о любых инцидентах безопасности.

5. Классификация Информации

Информация классифицируется по уровню важности и требуемому уровню защиты:

- **Публичная**: Информация, доступная для всех.
- **Внутренняя**: Информация, доступная только сотрудникам организации.
- **Конфиденциальная**: Информация, доступная ограниченному числу сотрудников и требующая защиты от несанкционированного доступа.
- **Секретная**: Информация критической важности, доступ к которой строго ограничен.

6. Управление Активами

6.1 Учет Активов

- Все активы должны быть учтены и идентифицированы.
- Назначается ответственный за каждый актив.

6.2 Защита Активов

- Физическая и логическая защита активов.
- Регулярное обновление и патчинг программного обеспечения.

7. Доступ и Управление Доступом

- Разграничение доступа на основании роли и необходимости.
- Использование многофакторной аутентификации.
- Регулярный пересмотр прав доступа.

8. Обучение и Осведомленность

- Обучение сотрудников правилам работы с информацией и активами.
- Проведение регулярных тренингов по безопасности.

9. Реагирование на Инциденты

- Процедуры обнаружения, сообщения и расследования инцидентов безопасности.
- Меры по устранению последствий инцидентов и предотвращению их повторного возникновения.

10. Мониторинг и Аудит

- Регулярный мониторинг использования информационных систем и активов.
- Проведение внутренних и внешних аудитов безопасности.

11. Обновление Политики

- Пересмотр и обновление политики как минимум один раз в год или при значительных изменениях в организации.

12. Нарушения и Дисциплинарные Меры

- Определение мер воздействия за нарушения политики, включая дисциплинарные взыскания вплоть до увольнения.

13. Заключение

Эта политика является обязательной для всех сотрудников и партнеров ТОО «Компания Э-КОМ ПРАЙМ». Все должны быть ознакомлены с политикой и следовать ее положениям для обеспечения безопасности и защиты информации и активов организации.

Information and Associated Assets Policy

1. Introduction

This policy establishes the rules and procedures for managing information and associated assets in TOO «Company E-COM PRIME». Its aim is to ensure the confidentiality, integrity, and availability of information and to protect assets from various threats and incidents.

2. Scope

The policy applies to all employees, contractors, partners, and other parties with access to the information and assets of TOO «Company E-COM PRIME».

3. Definitions

- **Information**: All data stored in electronic or physical form that has value to the organization.
- **Assets**: Equipment, software, information systems, documents, and other resources used for processing, storing, and transmitting information.

4. Roles and Responsibilities

- **Management**: Ensure policy implementation and allocate necessary resources.
- **IT and Security Department**: Develop and implement procedures for information protection and asset management.
- **Employees**: Adhere to established rules and procedures and report any security incidents.

5. Information Classification

Information is classified by its level of importance and required level of protection:

- **Public**: Information available to everyone.
- **Internal**: Information available only to the organization's employees.
- **Confidential**: Information available to a limited number of employees and requiring protection from unauthorized access.
- **Secret**: Critical information with strictly limited access.

6. Asset Management

6.1 Asset Inventory

- All assets must be recorded and identified.
- A responsible person must be assigned for each asset.

6.2 Asset Protection

- Physical and logical protection of assets.
- Regular updates and patching of software.

7. Access and Access Management

- Access control based on role and necessity.
- Use of multi-factor authentication.
- Regular review of access rights.

8. Training and Awareness

- Training employees on rules for handling information and assets.
- Regular security awareness training.

9. Incident Response

- Procedures for detecting, reporting, and investigating security incidents.
- Measures to mitigate the effects of incidents and prevent recurrence.

10. Monitoring and Audit

- Regular monitoring of information systems and asset usage.
- Conducting internal and external security audits.

11. Policy Update

- Review and update the policy at least once a year or in case of significant organizational changes.

12. Violations and Disciplinary Measures

- Define measures for policy violations, including disciplinary actions up to termination.

13. Conclusion

This policy is mandatory for all employees and partners of TOO «Company E-COM PRIME». Everyone must be familiar with the policy and adhere to its provisions to ensure the security and protection of the organization's information and assets.