INFORMATION SECURITY

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ТОО “HORIZON INC”

Настоящая политика определяет цели и задачи в области информационной безопасности (далее ИБ), устанавливает общие положения и требования в области ИБ.
Положения настоящей политики распространяется на все процессы и касается каждого сотрудника Компании;

Общие положения
Руководство Компании считает необходимым обезопасить свою деятельность в ходе протекания процессов в Компании с целью обеспечения конфиденциальности, сохранности и доступности информационных ресурсов Компании а также исправной и бесперебойной работы технических средств.
Задачи настоящей политики направлены на:

- Достижение целей в области качества, экологии, охраны труда и обеспечения безопасности труда;
- Соответственное и неприрывное протекание процессов ИСМ Компании;
- Реализацию принципов в области качества;
- Минимизацию рисков утраты, разглашения и утери информационных ресурсов;
- Снижение рисков отказа и поломки технических средств;

Объекты защиты
Деятельность Компании связана с:

- созданием и копированием интелектуальной собственности;
- оперированием сведений и документов содержащих коммерческую информацию,
- эксплуатацией технического оборудования в том числе персональных компьютеров, ноутбуков и оргтехники, использованием локальной сети для обмена информацией внутри Компании

В связи с чем, объекты информационной защиты можно разделить на:

- Информационные ресурсы;
- Технические средства и сетевые ресурсы.

Требования к объектам ИБ и способы их защиты

- Коммерческая информации должна быть конфиденциальна. Защита сведений и документов содержащих коммерческую информацию обеспечивается путем подписания каждым работником обязательство о неразглашении сведений, относящихся к коммерческой тайне;
  Интелектуальная собственность должна быть недоступна для посторонних субъектов. Материалы в электронном и бумажном виде являющиеся интелектуальной собственностью должны быть защищены паролями, должны быть ограниченными от несанкционированного доступа;
- Переносные накопители данных содержащие информационные активы должны быть защищены от копирования. Электронные носители данных содержащие информационные ресурсы, при необходимости должны быть защищены от несанкционированного копирования, изменения или удаления данных;
  Все персональные компьютеры подлежат защите, путем установления на них антивирусных программ;
- Для безопасной работы в локальной сети Компании предусматривается аутентификация пользователей с ограничением доступа к информационным ресурсам;
- Для безопасной работы в сети интернет предусматриваются способы ограничения доступа к опасным и нежелательным интернет-ресурсам;
- Для обеспечения беспрерывной работы а также для предотвращения утраты информации все технические средства на которых обрабатывается и хранится информация должны быть подключены к источникам бесперебойного питания.

Ответственность
Сотрудники Компании несут персональную ответственность за соблюдение требований изложенных в настоящей политике и обязаны сообщать о выявленныхнарушениях в области ИБ.

Генеральный Директор
ТОО «HORIZON INC»
Бакытбек Малик
15-05-2023

Horizon INC
БСН/БИН
070340001902

INFORMATION SECURITY

INFORMATION SECURITY POLICY

HORIZON INC POLICY

This Policy defines the goals and objectives in the field of information security and establishes HORIZON INC, LLP, (hereinafter referred to as the Company), general provisions and requirements in the field of information security.
The provisions of this policy apply to all Company processes and to each Company employee.

General Provisions
The Company considers it necessary to protect its activities during the implementation of Integrated Management System (hereinafter referred to as IMS) processes to ensure the confidentiality, integrity and availability of Company's information assets, as well as to ensure availability and uninterrupted operation of technical equipment.
This Policy has the following Objectives:

- Achieve quality, environment, health and occupational safety goals;
- Properly and continuously implement Company's IMS processes;
- Implement quality principles;
- Minimize the risk of disclosure or loss of information resources;
- Reduce the risks of failure and breakage of technical equipment processing and storing information resources.

Objects to be protected
The Company's activity on rendering educational and consulting services and their supportive processes is accompanied by:

- the creation and reproduction of materials being the intellectual property of the Company,
- handling information and documents containing business information
- operation of technical equipment, including personal computers, laptops and office equipment, use of local area network for information exchange within the Company.

Objects of information security can be:

- Information resources;
- Hardware and network resources

Requirements to Information Security objects and methods of their protection

- Commercial information shall be kept confidential. Data and documents containing business information shall be protected by signing an obligation by each employee not to disclose commercial classified information;
- Intellectual property shall be inaccessible to outsiders. Materials in electronic and paper form being the intellectual property shall be protected by passwords and restricted from unauthorized access;
- Portable data storage devices containing information assets and to be handed over to external users shall be protected from unauthorized data copying, modifying, or deleting;
- All personal computers shall be protected by anti-virus software;
- For safe operation of the company's local network, user authentication is provided with limited access to information resources ;
- For safe operation in Internet, access to dangerous and undesirable Internet resources is limited;
- To ensure continuous operation and to prevent loss of information, all hardware that processes and stores information shall be connected to UPS (Uninterrupted Power Supply).

Responsibility
Company employees are personally responsible for complying with the requirements set out in this policy and are obliged to report information security violations.

General Director
«HORIZON INC» LLP
Malik Bakytbek
15-05-2023