1. ПРЕДНАЗНАЧЕНИЕ

Политиката за информационна сигурност на ОмегаСофт ООД, заедно с прилежащите й политики, процедури и инструкции, дефинира изискванията за работа с информационните активи (ИА) на дружеството, целящи гарантирането на сигурността, наличността и цялостността на информацията.

2. ОБХВАТ

Политиката обхваща всички информационни активи на дружеството, в това число:

- Данни - всички документи (хартиени, оптични, магнитни, електронни или др.);
- Софтуер - всички закупени или наети програми, включително операционни системи или друг системен или приложен софтуер;
- Компютърно оборудване– всички сървъри, настолни и преносими компютри, мобилни устройства, IP телефони;
- Инфраструктурни системи и оборудване – мрежово активно и пасивно оборудване, климатизиращи системи и други сградни инсталации (електрозахранване, сигнално охранителна и система за контрол на достъпа), помещения за оборудване и персонала;
- Офис оборудване – принтери и многофункционални устройства, устройства за унищожаване на хартиени и електронни носители на информация;
- Персонал, договори с доставчици на стоки и услуги, консултанти, дилъри и клиенти;
- Физически помещения офиси на дружеството и наети помещения в център за данни
- Бизнес процеси - проектиране, разработване, внедряване и поддръжка на икономически софтуер.

3. ЦЕЛ

С настоящата политика за информационна сигурност, Ръководството на дружеството цели:

- Да осигури непрекъснатост на бизнес процесите;
- Да минимизира рисковете от неоторизиран достъп и неправомерна употреба на ИА на дружеството;
- Да минимизира потенциалните загуби и вреди при пробив в информационната сигурност;
- Да информира служителите на дружеството за техните задължения, свързани с информационната сигурност;

4. СТРУКТУРА

Политиката за информационна сигурност се съдържа в следните документи:

- Политика за чисто работно място и чист екран;
- Политика за управление на непрекъснатостта на бизнеса;
- Политика за паролите;
- Политика за управление на промените;

- Политика за управление на обновленията;
- Политика за допустима употреба на ИА;
- Политика за резервно копиране и възстановяване на информацията;
- Политика за защита от зловреден код;
- Политика за класификация на ИА;
- Политика за управление на инциденти;
- Политика за мониторинг и работа с ИА;
- Политика за контрол на достъпа;
- Политика за управление на риска;
- Политика за работа с мобилни устройства и мобилни носители на информация;
- Политика за измерване на ефикасността на механизмите за контрол;
- Вътрешни правила за трудов ред

5. ДЕФИНИЦИИ И СЪКРАЩЕНИЯ

- ИА – информационни активи (виж раздел 2)
- Собственик на ИА – роля, която се назначава индивидуално за всеки отделен ИА. Изпълнява се от служител на дружеството, който участва в бизнес процеси и има задълбочени познания относно информацията в съответния ИА. На него са делегирани следните права и задължения: да организира и наблюдава събирането и организацията на данните, да администрира контрола на достъп до ИА, да оценява риска за пряко свързаните бизнес процеси, да предприема мерки за намаляване на риска, да класифицира зачислените му активи;
- Системен администратор на ИА – индивидуална роля, свързана с оперативните дейности извършвани по поддръжката на всеки отделен ИА. ИТ администратора може да делегира конкретни дейности свързани с поддръжката на поверените му ИА, но не може да делегира отговорността за тях;
- Потребител – роля свързана с използването на конкретен ИА. Потребителят е лице, което след потвърждаване на самоличността, получава достъп до конкретна информация и/или функционалност от конкретния ИА. Освен служители на дружеството, достъп до ИА може да бъде предоставян и на външни лица, като потвърждаването на самоличността им може да става както чрез име и парола, така и чрез други методи, специфицирани за конкретния ИА.

6. ОТГОВОРНОСТИ

За спазването и изпълнението на политиката на информационна сигурност отговарят всички служители на ОмегаСофт ООД и конкретно:

- Управителят на дружеството обявява собственик и системен администратор за всеки ИА съгласно Политика за класификация на ИА;
- Управителят на дружеството – контролира развитието на системата за управление на сигурността на информацията, приема докладите за оценка на риска, както и взима отношение при инциденти или въпроси свързани с информационната сигурност;
- Собствениците на ИА – отговарят за съблюдаването на политиката за сигурност на информацията при изпълняване на дейностите свързани с поверените им ИА.
- Системен администратор – участва в развитието на системата за управление на сигурността на информацията, отговаря за анализа на риска за сигурността на информацията, извършва контролирани тестове с цел оценка на сигурността и предоставя резултатите от тези тестове на ИТ Директор. Също така отговаря и за оперативното управление на достъпа до поверените му ИА съгласно разпореждането на съответните собственици на ИА, за поддържането на ИА съгласно изискванията на политиката за информационна сигурност и за разследване на всеки сигнал свързан със информационната сигурност.
- Потребители на ИА– отговарят за използването на ИА според изискванията на политиката за сигурност на информацията. Потребителите са задължени да сигнализират за всички проблеми или инциденти свързани с информационната сигурност.

7. КОНТРОЛ

Изпълнението на тази политика и произлизащите от нея документи, се контролира непрекъснато от Ръководството и всички служители на дружеството, съгласно дефинираните им отговорности. Проверка и актуализация на документите се извършва не по-малко от веднъж годишно, след с ръководството, както и при предложение или инцидент свързан с информационната сигурност.

8. САНКЦИИ

При умишлено неспазване на политиката за сигурност на информацията или проява на небрежност по отношение на нейните разпоредби, на провинилите се служители се налагат дисциплинарни наказания в съответствие с Кодекса на Труда и в зависимост от тежестта на провинението е възможно да се инициира съдебно производство.