“ ТРАНСРЕМОНТСТРОЙ” ЕАД

Строителство и ремонт на подземен и надземен (трамваен) релсов път. Производство, монтаж и ремонт на съоръжения и резервни части , стандартни и нестандартни изделия от метал, метални конструкции и елементи от нея. Заготовка на армировъчна, кангална, гладка и оребрена на пръти стомана.Събиране,съхраняване, преработка и предаване за последващо третиране на черни и цветни метали. Поддръжка и отдаване под наем на собствен кофраж, кофражни детайли и елементи за строително-монтажни дейности

Утвърдил: .....
Юлиана Мерджанова
Изпълнителен директор
Дата: 10.05.2018г.

ПОЛИТИКА

ПО ЗАЩИТА НА ЛИЧНИ ДАННИ

Ръководството на ТРАНСРЕМОНТСТРОЙ ЕАД, в лицето на Изпълнителния директор, официално декларира своите Политики по защита на лични данни на информационните ресурси в обхвата на дейността си.

Политиката е документирана, огласени и разбрани от всички служители, които имат достъп до информацията и защитата на лични данни в ТРАНСРЕМОНТСТРОЙ ЕАД. Политиките са одобрени от Изпълнителния директор и се прилагат в рамките на цялото дружество. Политиката се поддържа от Изпълнителен директор и длъжностно лице по защита на лични данни".

Настоящата политика по защита на лични данни задава рамката на система от мерки, насочени към:

1. Гарантиране на конфиденциалност на информацията, чрез прилагането на одобрени ограничения върху достъпа и разкриването на информация;
2. Спазване на принципите по защита на лични данни;
3. Осигуряване на цялостност на информацията, чрез защита срещу неправомерни изменения или разрушаване на информация;
4. Осигуряване на достъпност на информацията, чрез осигуряване на надежден и навременен достъп на информацията;
5. Постигане на отчетност на информацията, чрез въвеждане на контрол върху достъпа и правата върху информационните ресурси.

Обхват на системата за управление на информационната сигурност:

Строителство и ремонт на подземен и надземен (трамваен) релсов път. Производство, монтаж и ремонт на съоръжения и резервни части , стандартни и нестандартни изделия от метал, метални конструкции и елементи от нея. Заготовка на армировъчна, кангална, гладка и оребрена на пръти стомана.Събиране,съхраняване, преработка и предаване за последващо третиране на черни и цветни метали. Поддръжка и отдаване под наем на собствен кофраж, кофражни детайли и елементи за строително-монтажни дейности

Териториален обхват:

Системата за управление на информационната сигурност обхваща централния офис на ТРАНСРЕМОНТСТРОЙ ЕАД, в сградата на ул. Джерман № 7 в гр. София и офис сграда на територията на Елаците Мед АД в гр. Етрополе.

Обхват на процесите:

Системата за управление на информационната сигурност обхваща следните процеси:

1. Приемане и обработване на входящи и изходящи документи /външни и вътрешни/;
2. Приемане, обработване, отпечатване на договори /клиенти, доставчици/;
3. Извеждане на справки за служителите и периодично архивиране и съхранение на електронната и хартиена информация и досиета свързани с тях;
4. Изготвяне на финансови отчети;

Обхват на информационните ресурси:

Системата за управление на информационната сигурност обхваща цялата документирана информация (в електронен вид и на хартия), намираща се или касаеща:

1. Връзки с клиенти;
2. Връзка с доставчици;
3. Бази данни;
4. Компютри, в т.ч. преносими;
5. Софтуерни активи;
6. Локална мрежа- INTRANET
7. Електронната страница на група ГЕОТЕХМИН;
8. Носители на информация (дискове, USB памети и др.);
9. Устройства за копиране и предаване на данни;
10. Мобилни устройства;
11. Инфраструктура на ТРАНСРЕМОНТСТРОЙ ЕАД (електрозахранване, кабели за локална мрежа и др.);
12. Персонал.

Целите на настоящата политика са:

1. Осигуряване на непрекъснатост на БИЗНЕС ПРОЦЕСИТЕ;
2. Минимизиране на рисковете за защита на личните данни, причиняващи загуби или вреди на субектите на данни и на ТРАНСРЕМОНТСТРОЙ ЕАД, като администратор на лични данни, нейните клиенти, партньори и други заинтересовани страни;
3. Минимизиране на степента на загуби или вреди, причинени от пробиви в информационната сигурност;
4. Осигуряване на необходимите ресурси за внедряване на ефективна система за управление;
5. Информиране на служителите за техните отговорности и задължения по отношение на информационната сигурност;
6. Осигуряване на съответствие с нормативни и договорни изисквания.

Ръководството на ТРАНСРЕМОНТСТРОЙ ЕАД ще прилага следните основни принципи при разработване, внедряване и поддържане на системата:

1. Спазване изискванията на законите
2. Спазване на принципите за защита на лични данни;
3. Защита на данни и неприкосновеност на лична информация;
4. Опазване на архивите на организацията;
5. Защита на авторски права, търговска информация и други права върху интелектуална собственост.
6. От общоприетите най-добри практики за защита на лични данни:
7. Разработване на политика по защита на лични данни;
8. Разпределяне на отговорностите по защита на лични данни;
9. Обучение по защита на лични данни;
10. Докладване на инциденти, свързани със сигурността;

11. Управление непрекъснатостта на работа;

12. Дисциплинарен процес вследствие от нарушенията на политиката по сигурността.

Усилията на ръководството са насочени към:

1. Критичната (чувствителната) информация, като лични данни и системи да бъдат подлагани на редовен анализ на риска;

2. За критичните (чувствителни) информационни ресурси и системи да бъдат определени „собственици" - служители отговорни за конкретните бизнес приложения, компютри и мрежи;

3. Информацията да бъде класифицирана по начин, който показва нейната критичност и чувствителност по отношение на организацията;

4. Персоналът да осъзнава проблемите на защитата на лични данни;

5. Организацията да се съобразява с лицензите за софтуер, авторските и други свързани права, както и с други правни, регулаторни и договорни задължения;

6. Нарушаването на политиката по защитата на лични данни и евентуалните недостатъци в системата за защита на лични данни да бъдат докладвани;

7. Информационните ресурси да бъдат защитавани от гледна точка на изискванията за конфиденциалност, цялостност и достъпност.

Въвеждането и спазването на политиката по защита на лични данни цели да се забранят:

1. Използването на информацията и системите на организацията без оторизация или за цели, които не са свързани с дейността й;

2. Изнасяне на оборудване или информация от офисите и производствените помещения на организацията без оторизация;

3. Неоторизирано копиране на информация и софтуер;

4. Компрометиране на пароли (например със записване или разпространяване);

5. Използване на персонална информация за бизнес цели, освен ако няма изрична оторизация;

6. Фалшифициране на доказателства в случай на инцидент.

7. Дискриминационни или нападателни изявления и обявяване на лични данни които могат да бъдат противозаконни (например с използване на електронна поща или интернет);

8. Разпространение на незаконни материали (например с неприлично или дискриминационно съдържание и с лични данни).

Отговорности:

За осъществяване на настоящата политика и за осигуряване функционирането на системата за управление, Ръководството определя следните отговорности на:

Изпълнителният директор и ръководител отдел Човешки ресурси, СУ и административни дейности

Формулират, преглеждат и представят за одобрение Политиката по защита на лични данни и контролират ефикасността на нейното изпълнение;

1. Планират необходимите ресурси за сигурността на информационната система;

2. Определят ролите и отговорностите свързани със сигурността на информацията, изготвят планове за обучение ;

3. Координират прилагането на мерки за защита на информационната сигурност.

Доставчиците за ИТ услуги, наречени за краткост Системен/ни администратор/и:

1. Отговарят за управление и поддържане на интернет, електронна поща, сървъри, локална мрежа, архивиране, техническа защита (софтуер и хардуер) от вреден софтуер;
2. Нива на достъп;
3. Проследимост на включване и опити за включване;
4. Изготвяне и поддръжка на цялостната документация, свързана с администрирането на информационната система и нейните подсистеми.
5. Координира дейностите по прилагане на Политиката и мерките по осигуряване на защита на лични данни;
6. Отговаря за изготвяне на методика за оценка на риска и за класификация на информацията;
7. Извършва оценка на риска и адекватност на мерките при изменения в информационната система;
8. Управлява възникнали несъответствия и инциденти;
9. Съдейства за осигуряване на обучението и осъзнаването на потребителите на информационната система.

Потребители:

1. Потребителите на информационната система, се задължават да следват политиките, фирмените стандарти и инструкциите по защита на лични данни, да докладват за проблеми и инциденти в информационната система.

Оценка на риска

1. Оценката на риска се прилага за всеки актив на ТРАНСРЕМОНТСТРОЙ ЕАД, информационна система и включва приложения, сървъри, мрежата, и всеки процес или фирмен стандарт, чрез които системата се администрира и/или поддържа.
2. Идентифицирането и оценката на риска се извършват на базата на разработена и внедрена в ТРАНСРЕМОНТСТРОЙ ЕАД, **РП 1-1 „Оценка на риска и възможностите на бизнес процесите и защитата на лични данни“**

Методика за оценка на риска

1. Критериите за оценка на риска се базират на вероятността даден източник на заплаха да се възползва от определена потенциална уязвимост и да окаже въздействие върху организацията.
2. За да се определи вероятността да се случи неблагоприятно събитие се анализират заплахите за Информационната система заедно с потенциалните уязвимости и съществуващи мерки.
3. Въздействието се отнася до степента на вреда, която може да бъде причинена от проявата на уязвимостта.
4. Резултатите от оценката на риска определят мерките за контрол за намаляване на риска в съответствие с нивата на риска.

5. Оценката на риска се извършва минимум веднъж годишно, за да бъдат отчетени измененията в изискванията за сигурност, активите, заплахите, уязвимостите, въздействията или други настъпили промени. При необходимост се извършва незабавно.
6. Изпълнението на политиката по оценка на риска е отговорност на Работна група.

Вътрешна организация на защитата на лични данни.

Ръководството провежда политика за координиране на цялата дейност в организацията по внедряването и поддържането на мерките за защита.

1. Ръководството на ТРАНСРЕМОНТСТРОЙ ЕАД е извършило разпределяне на отговорностите по защита на лични данни в съответствие с Политиката по защита на лични данни. Ангажиментите на служителите са дефинирани в длъжностните им характеристики.
2. Координирането на дейностите по отношение на защитата на лични данни е възложено на длъжностно лице по защита на лични данни.