Политика за реакция при нарушаване на данни

Дата: 01/03/2021

Версия 1.0

Община: Борован

Съдържание

1 Цел

Целта на политиката е да установи целите и визията за процеса на реагиране при нарушаване. Тази политика ясно ще определи за кого се прилага и при какви обстоятелства и ще включва определението за нарушение, ролята и отговорностите на персонала, стандартите и показателите (например, за да се даде възможност за приоритизиране на инцидентите), както и за докладване, коригиране и механизми за обратна връзка. Политиката трябва да бъде добре разгласена и да бъде лесно достъпна за целия персонал, чиито задължения включват защита на личния живот на данните и защита.

Намеренията за информационна сигурност за публикуване на Политика за реакция на нарушения на данните са да насочат значително внимание към сигурността на данните и нарушенията на сигурността на данните и как установената култура на откритост, доверие и почтеност на Община Борован трябва да реагира на такава дейност. Информационната сигурност се ангажира да защитава служителите, партньорите от незаконни или вредоносни действия от страна на физически лица, съзнателно или несъзнателно.

1.1 Обща информация

Тази политика налага на всяко физическо лице, което подозира, че е настъпила кражба, нарушение или излагане на Община Борован Защитени данни или Чувствителни данни, трябва незабавно да предостави описание на случилото се по електронната поща на Helpdesk @ <вашият имейл адрес> , като се обадите на < Борован тел. Номер> или чрез използването на уеб страницата за отчитане на информационното бюро на http: // <ИМЕТО НА ОРГАНИЗАЦИЯ>. Този имейл адрес, телефонен номер и уеб страница се контролират от Администратора на информационната сигурност на Община Борован, този екип ще проучва всички докладвани кражби, нарушения на данните за да потвърди дали е извършена кражба, нарушение или излагане на конфиденциална информация. Ако е настъпила кражба, нарушение или излагане на конфиденциална информация, администраторът по сигурността на информацията ще следва съответната процедура.

2 Обхват

Тази политика се прилага за всички, които събират, осъществяват достъп, поддържат, разпространяват, обработват, защитават, съхраняват, използват, предават, изхвърлят или обработват по друг начин лична информация на Община Борован. Всички споразумения с доставчици ще съдържат подобен език, който защитава фонда.

В случай на кражба, нарушение на данните на Община Борован, бъдат идентифицирани, процесът на премахване на целия достъп до този ресурс ще започне.

<Кмет или зам. Кмет> ще председателства екип за реагиране на инциденти, който ще се справи с нарушението.

Екипът ще включва членове от:

- ИТ инфраструктура
- Финанси (ако е приложимо)
- Правна
- Комуникации
- Човешки ресурси
- Отдел, който използва съответната система и чиито данни може да са нарушени или изложени.
- Допълнителни отдели въз основа на съответния тип данни, лица, които сметне за необходимо от Председателя.

При потвърдени кражби, нарушения или излагане на данни на Община Борован.

<Кмет или зам. Кмет> ще бъде уведомен за кражба, нарушение или излагане на конфиденциална информация. ИТ Отдела заедно с определения криминален екип ще анализират нарушението, за да определят първопричината.

3 Разработете комуникационен план.

Работете с отделите на Община Борован за комуникации, правни и човешки ресурси, за да решите как да съобщите нарушението на: а) вътрешни служители, б) обществеността и в) пряко засегнатите.

4 Собственост и отговорности

Роли и отговорности:

- Спонсори - Спонсорите са онези членове на Община Борован, които носят основната отговорност за поддържането на конкретен информационен ресурс. Спонсорите могат да бъдат назначени от всяко изпълнително ръководство във връзка с техните административни отговорности или чрез действителното спонсорство, събиране, разработване или съхранение на информация.
- Администратор на информационната сигурност е онзи служител на Община Борован, определен от <Кмет или зам. Кмет> или директора по инфраструктурата на информационните технологии (ИТ), който

осигурява административна подкрепа за прилагането, надзора и координацията на процедурите и системите за сигурност по отношение на конкретни информационни ресурси след консултация със съответните Спонсори.

- Потребителите включват почти всички членове служители на Община Борован до степента, до която имат разрешен достъп до информационни ресурси, и могат да включват персонал, попечители, изпълнители, консултанти, стажанти, временни служители и доброволци.
- Екипът за реагиране на инциденти се ръководи от <Кмет или зам. Кмет> и включва, но не се ограничава до, следните отдели или техни представители: ИТ-инфраструктура, ИТ-приложения; съобщения; Правна; Финансови услуги; Човешки ресурси.

5 Изпълнение

Всеки служител на Община Борован, установен в нарушение на тази политика, може да бъде обект на дисциплинарни мерки, включително до прекратяване на работата. Всяка трета страна партньорска компания, установена в нарушение, може да прекрати мрежовата им връзка.

6 Определения

Шифроване или криптирани данни - най-ефективният начин за постигане на сигурност на данните. За да прочетете криптиран файл, трябва да имате достъп до секретен ключ или парола, които ви позволяват да го декриптирате. Некриптираните данни се наричат обикновен текст;
Обикновен текст - Некриптирани данни.
Хакер - термин от жаргона за компютърен ентусиаст, т.е. човек, който се радва на изучаване на програмни езици и компютърни системи и често може да се счита за експерт по темата.
Лична информация - Всякакви данни, които потенциално могат да идентифицират конкретно лице. Всяка информация, която може да се използва за разграничаване на един човек от друга и може да се използва за деанонимизиране на анонимни данни, може да се счита за такава
Информационен ресурс - Данните и информационните активи на организация, отдел или звено.
Предпазни мерки - въведени противодействия, контрол за избягване, откриване, противодействие или минимизиране на рисковете за сигурността на физическа собственост, информация, компютърни системи или други активи. Защитните мерки помагат да се намали рискът от повреда или загуба чрез спиране, възпиране или забавяне на атака срещу актив.
Чувствителни данни - Данни, които са криптирани или в обикновен текст и съдържат лична или конфиденциална информация.