НОТАРІАЛЬНА ПАЛАТА УКРАЇНИ

КОМІСІЯ З ПИТАНЬ ІНФОРМАТИЗАЦІЇ, ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ТА ЗАПОБІГАННЯ КІБЕРЗЛОЧИННОСТІ

ІНФОРМАЦІЙНИЙ ЛИСТ №1-4/2024

ЩОДО ЗБЕРЕЖЕННЯ ЕЛЕКТРОННОЇ (ЦИФРОВОЇ) ІНФОРМАЦІЇ НОТАРІУСА ІЗ ВИКОРИСТАННЯМ ПРАВИЛА 3-2-1

Відповідно до статті 8 Закону України «Про нотаріат» нотаріальна таємниця – сукупність відомостей, отриманих під час вчинення нотаріальної дії або звернення до нотаріуса заінтересованої особи, в тому числі про особу, її майно, особисті майнові та немайнові права і обов'язки тощо.

НОТАРІУСИ ПРАЦЮЮТЬ З ІНФОРМАЦІЄЮ, яка має обмежений доступ, містить персональні дані та дані, що охороняються нотаріальною таємницею. Такі дані можуть бути **У ПАПЕРОВІЙ, АБО ЕЛЕКТРОННІЙ ФОРМІ**.

У сучасному цифровому світі нотаріуси розраховують на свої напрацювання - електронні документи, бази даних та інші цифрові активи більше, ніж будь-коли раніше. Втрата цих даних може негативно вплинути на робочий процес, призвести до юридичних наслідків, включаючи фінансові збитки, шкоду для ділової репутації, порушення конфіденційності клієнтів тощо.

Як показують сучасні реалії професійної діяльності нотаріуса: комп'ютер, як робочий інструмент нотаріуса, може бути вилучений в рамках кримінального провадження, можуть бути викрадений, також комп'ютери можуть бути пошкоджені внаслідок атаки ворога, через природні катастрофи (пожежі, повені), а також хакерські атаки тощо. Будь що з вище перерахованого може призвести до пошкодження, знищення (втрати) даних.

БЕЗПЕКА ДАНИХ – ЦЕ ПРОЦЕС ЗАХИСТУ конфіденційності, цілісності та доступності даних від несанкціонованого доступу, втрати, пошкодження або розкриття.

ЗАСОБИ, які у комплексі дають найкращі результати для **забезпечення належного рівня безпеки цифрових даних** – це:

1) Шифрування даних
2) Багаторівнева система доступу до даних
3) Резервне копіювання
4) Використання антивірусного програмного забезпечення

У цьому листі ми розглянемо Резервне копіювання, як ефективний засіб забезпечення безпеки даних, з метою зменшення ризику їх втрати.

Своєчасне та якісне резервне копіювання даних допомагає захистити інформацію, уникнути юридичних проблем та забезпечити безперебійну роботу.

РЕЗЕРВНЕ КОПІЮВАННЯ ЗА ПРАВИЛОМ 3-2-1 – це надійний і перевірений метод захисту даних від втрати чи пошкодження.

ЩО ТАКЕ ПРАВИЛО 3-2-1?

Правило грунтується на трьох простих, але важливих принципах:
- ***Створіть три копії даних***: це гарантує, що у вас буде резервна копія, навіть якщо одна або дві інші копії будуть втрачені або пошкоджені;
- ***Зберігайте створені копії на двох різних типах носіїв інформації (наприклад комп'ютер та окремо зовнішній накопичувач (флешка)***: це захистить ваші дані від пошкоджень, які можуть виникнути через відмову одного типу носія;
- Завжди ***зберігайте одну копію даних у захищеному і надійному місці, окремо від інших копій***: це забезпечить додатковий рівень захисту ваших даних.

ПЕРЕВАГИ ВИКОРИСТАННЯ ПРАВИЛА 3-2-1 ДЛЯ НОТАРІУСІВ:
- *Захист даних*: правило 3-2-1 збільшує шанси на те, що ваші дані не будуть остаточно втрачені, навіть у разі серйозної загрози (події).
- *Зменшення часу для відновлення діяльності*: втрата даних може призвести до простою, перешкоджаючи вашій роботі та спричинити фінансові та репутаційні втрати.
- *Відповідність нормативним вимогам*: нотаріуси зобов'язані захищати конфіденційність клієнтів та дотримуватися вимог законодавства.
- *Спокій*: знання того, що ваші дані захищені, забезпечить душевний спокій.

РЕАЛІЗАЦІЯ ПРАВИЛА 3-2-1 ДЛЯ НОТАРІУСІВ:

Крок 1. Визначте важливі для вас електронні (цифрові) дані:

- проаналізуйте, які типи електронних документів (файлів), баз даних та іншої інформації, що ви створили, створюєте, зберігаєте та використовуєте у своїй нотаріальній діяльності, необхідно захистити від втрати;

- дані, які містять конфіденційну інформацію, персональні дані осіб чи містять нотаріальну таємницю, не рекомендуємо зберігати на носіях інформації у відкритому вигляді (без шифрування);

- визначте, з якою періодичністю ці дані оновлюються/змінюються, щоб визначити потрібний графік резервного копіювання.

Крок 2. Виберіть носії для зберігання резервних копій:

- Носієм для першої копії ваших даних може бути робочий комп'ютер на якому вони безпосередньо обробляються і використовуються;

- Друга копія може бути розміщена в межах офісу на окремому комп'ютері або на зовнішньому жорсткому диску (флешці), або на локальному мережевому сховищі даних (NAS);

- Третя копія може розміщуватись, аналогічно другій, на зовнішньому жорсткому диску (флешці), комп'ютері, NAS тощо, але важливо щоб така копія зберігалася в іншому надійному місці. Для третьої або наступної копії можна використовувати надійні хмарні файлові сховища

Обираючи хмарне сховище, важливо врахувати кілька факторів, таких як надійність, безпека, доступність простору, простота використання та ціна. Ось декілька з надійних хмарних сховищ, які можна згадати:

pCloud:

- Швейцарський хостинг: pCloud відомий своєю прихильністю до конфіденційності та дотримується суворих швейцарських законів про захист даних.
- Шифрування: Пропонує шифрування на стороні клієнта AES 256, що гарантує, що ваші дані будуть зашифровані до того, як вони покинуть ваш пристрій.
- Безпека: pCloud регулярно проходить незалежні аудити безпеки.

- Функціональність: Доступні безкоштовні та платні плани з різними обсягами пам'яті, а також додаткові функції, такі як синхронізація файлів, спільний доступ до файлів та резервне копіювання.

IDrive:

- Шифрування: Пропонує шифрування на стороні клієнта AES 256 та шифрування на стороні сервера AES 256 для додаткового рівня безпеки.
- Резервне копіювання: IDrive пропонує широкий спектр можливостей резервного копіювання, включаючи резервне копіювання комп'ютера, сервера, мобільного пристрою та соціальних мереж.
- Функціональність: Доступні безкоштовні та платні плани з різними обсягами пам'яті, а також додаткові функції, такі як синхронізація файлів, спільний доступ до файлів та відновлення файлів.
- Надійність: IDrive має багаторічний досвід роботи та зарекомендував себе як надійний постачальник хмарних сховищ.

Backblaze:

- Необмежене сховище: Backblaze пропонує необмежене сховище за фіксованою річною платою, що робить його вигідним варіантом для користувачів, яким потрібна велика кількість місця.
- Просте використання: Backblaze відомий своїм простим інтерфейсом та легкістю використання.
- Надійність: Backblaze має 99,99% гарантії uptime та пропонує функцію відновлення даних, яка допоможе вам відновити файли у разі їх видалення або пошкодження.

Dropbox:

- Широке поширення: Dropbox є одним із найпопулярніших хмарних сховищ у світі, що робить його зручним для спільного використання файлів з іншими.
- Простота використання: Dropbox має простий інтерфейс та доступний з будь-якого пристрою.
- Функціональність: Доступні безкоштовні та платні плани з різними обсягами пам'яті, а також додаткові функції, такі як синхронізація файлів, спільний доступ до файлів та контроль версій.

Google Drive:

- Інтеграція з Google: Google Drive добре інтегрується з іншими службами Google, такими як Gmail та Google Docs.
- Безкоштовне сховище: Google Drive пропонує 15 ГБ безкоштовного сховища, що робить його гарним варіантом для початківців.
- Функціональність: Доступні безкоштовні та платні плани з різними обсягами пам'яті, а також додаткові функції, такі як синхронізація файлів, спільний доступ до файлів та контроль версій.

OneDrive:

- Інтеграція з Microsoft: OneDrive добре інтегрується з іншими продуктами Microsoft, такими як Windows, Office 365.
- Це робить його зручним для користувачів Windows та тих, хто вже використовує інші продукти Microsoft.
- Безкоштовне сховище: OneDrive пропонує 5 ГБ безкоштовного сховища, що робить його гарним варіантом для початківців.
- Існує також можливість розширити сховище за допомогою платних планів.

- Функціональність: OneDrive пропонує широкий спектр функцій, таких як синхронізація файлів, спільний доступ до файлів, контроль версій, резервне копіювання та відновлення файлів.
- Безпека: OneDrive використовує шифрування AES 256 для захисту ваших даних.
- Компанія Microsoft також має суворі політики безпеки та конфіденційності.

Важливо зазначити, що це лише деякі з надійних хмарних сховищ.

Крок 3. Визначте політику створення резервних копій:

● визначте, як часто ви будете створювати резервні копії, враховуючи частоту оновлень даних, один раз на тиждень, один раз на місяць тощо, при цьому рекомендуємо визначити відповідальну особу за створення копій;

● можна автоматизувати процес створення копій за допомогою спеціального програмного забезпечення, що полегшить резервне копіювання.

Крок 4. Перевіряйте цілісність та працездатність резервних копій:

● періодично перевіряйте, чи можна відновити дані з носіїв (сервісів) на яких ви розмістили резервні копії ваших даних;

● періодично змінюйте паролі доступу до хмарних сховищ, на яких розміщуються резервні копії, обов'язково налаштуйте 2FA (двофакторна аутентифікація) для входу до таких сховищ.

Крок 5. Впроваджуйте і використовуйте додаткові заходи безпеки:

● за необхідності зашифруйте деякі резервні копії, це суттєво зменшить ризик витоку (розголошення) даних у разі їх крадіжки;

● обмежте фізичний доступ до носіїв (сервісів) на яких зберігаються резервні копії, носії інформації зберігайте у безпечних місцях;

● використовуйте різні паролі для всіх важливих облікових записів, як-от електронної пошти, хмарних сховищ, інтернет-банкінгу. Використовувати ті самі паролі небезпечно. Якщо хтось дізнається пароль для одного облікового запису, то зможе отримати доступ до інших;

● використовуйте безпечні сервіси електронної пошти, які мають функціонал попередньої перевірки електронних листів на шкідливий вміст;

● використовуйте постійно оновлюване антивірусне програмне забезпечення;

● регулярно встановлюйте оновлення операційної системи, а також оновлюйте інше програмне забезпечення.

Крок 6. Майте план відновлення після надзвичайних ситуацій:

● створіть детальний план дій для відновлення ваших даних у разі виникнення різних ситуацій - на випадок стихійного лиха, пожежі, крадіжки, поломки комп'ютера, або носія інформації, а також на випадок можливої кібератаки;

● визначте пріоритетність відновлення різних типів даних та послідовність дій;

● проводьте регулярні тренування з відновлення даних за цим планом.

Крок 7. Врахуйте ризики воєнного часу:

● завжди майте в наявності резервну копію даних на випадок, якщо терміново треба покинути офіс, або ж взагалі населений пункт;

● така копія має бути максимально повна, дані на ній мають бути максимально актуальні;

- рекомендуємо для такої копії використовувати хмарне сховище, адже це забезпечить вам збереження актуальних даних у безпечному місці, незважаючи на будь-які локальні загрози.

Ознайомившись з цими рекомендаціями та скориставшись ними практично, ви зможете мінімізувати ризики втрати ваших напрацювань та зможете швидко відновити їх у разі непередбачених обставин.

Перефразовуючи відому фразу, пам’ятаймо:
Культура поводження з інформацією з’їдає досвід та репутацію нотаріуса на сніданок!