



## **РОЗПОРЯДЖЕННЯ**

від 11 березня 2026 року

№ 31-в

Про затвердження Політики інформаційної безпеки в інформаційно-комунікаційних системах виконавчого комітету Миргородської міської ради

Відповідно до п. 20 ч. 4 ст. 42 Закону України «Про місцеве самоврядування в Україні», з метою забезпечення належного рівня захисту інформаційних ресурсів, підвищення ефективності управління інформаційною безпекою, запобігання загрозам несанкціонованого доступу до інформації; відповідно до Законів України «Про інформацію», «Про доступ до публічної інформації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основні засади забезпечення кібербезпеки України»; згідно з вимогами ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT) «Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги», ДСТУ ISO/IEC 27002:2023 (ISO/IEC 27002:2022, IDT) «Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки»:

1. Затвердити Політики інформаційної безпеки в інформаційно-комунікаційних системах виконавчого комітету Миргородської міської ради (додається).
2. Встановити, що Політика інформаційної безпеки виконавчого комітету Миргородської міської ради є обов'язковою до виконання посадовими особами виконавчих органів міської ради, які працюють з інформаційними ресурсами.
3. Керівникам виконавчих органів, посадовим особам виконавчого комітету Миргородської міської ради забезпечити неухильне дотримання затвердженої Політики.
4. Організацію виконання цього розпорядження покласти на відділ інформаційних технологій та комп'ютерного забезпечення (Нестефоренко Р.Ю.) та відповідального за організацію та забезпечення захисту інформації, а контроль за виконанням – на керуючу справами виконавчого комітету Нікітченко А.Б.

**Міський голова**

**Сергій СОЛОМАХА**

## **Політики інформаційної безпеки в інформаційно-комунікаційних системах виконавчого комітету Миргородської міської ради**

### **1. ВСТУП**

#### **1.1. Загальні положення**

Ця політика інформаційної безпеки визначає основні засади забезпечення належного рівня інформаційної безпеки виконавчого комітету Миргородської міської ради (далі – Політика). Політика служить центральним програмним документом з інформаційної безпеки (далі - ІБ), з яким повинні бути ознайомлені всі працівники виконавчого комітету Миргородської міської ради та постачальники послуг і визначає дії, застереження, заборони, яких повинні дотримуватися всі користувачі інформаційних та цифрових активів виконавчого комітету. Функцію відповідального за інформаційну безпеку виконує керівник виконавчого органу та відповідальний за організацію та забезпечення захисту інформації виконавчого комітету або інша особа, визначена належним чином.

Належний рівень інформаційної безпеки, це такий стан фізичного, інформаційного середовища та середовища користувачів інформаційних та цифрових активів виконавчого комітету Миргородської міської ради, який гарантує конфіденційність, доступність, цілісність інформації та спостережність і контрольованість систем/підсистем, в яких ця інформація циркулює.

Належний рівень інформаційної безпеки досягається за рахунок вмілого застосування комплексу програмних/технічних засобів та організаційних заходів, спрямованих на забезпечення захищеності даних від зловмисного використання.

Вимоги та обмеження Політики, застосовуються до мережевої інфраструктури, баз даних, носіїв інформації, засобів шифрування, друкованих документів, мультимедіа файлів, засобів бездротового зв'язку, телекомунікаційних систем, аудіо повідомлень та будь-яких інших засобів, що використовуються для передачі, обробки та зберігання інформації у всіх апаратних, програмних та інших інформаційних та цифрових системах виконавчого комітету. Цієї політики повинні дотримуватися всі штатні та тимчасові працівники в усіх місцях (на робочому місці, в адмінбудівлі чи працюючи віддалено), а також всі постачальники послуг, які працюють з виконавчим комітетом Миргородської міської ради.

### **2. ОБОВ'ЯЗКИ ПРАЦІВНИКІВ**

#### **2.1. Вимоги до працівників**

Першою лінією захисту в системі управління інформаційною безпекою є персонал або користувачі. Користувачі несуть відповідальність за безпеку всіх даних, які можуть надходити до них у будь-якому форматі.

Обов'язком всіх працівників виконавчого комітету є вжиття необхідних заходів для забезпечення фізичної безпеки активів. Якщо будь хто з працівників бачить невстановлену особу в службовому приміщенні чи приміщенні з обмеженим доступом, він/вона повинен вжити всіх можливих заходів для виведення такої особи із зазначеного приміщення та проінформувати про такий випадок відповідального за організацію та забезпечення захисту інформації.

Захист робочих станцій. Всі робочі станції (ПК), які знаходяться в установі не повинні залишати приміщення ради без відповідного дозволу керівника чи відповідального за організацію та забезпечення захисту інформації. Всім новим користувачам надається перший інструктаж на робочому місці щодо правил використання та зберігання робочих станцій. На ПК, які містять конфіденційні дані слід дотримуватися максимальної обережності, щоб ці дані не були скомпрометовані. При використанні робочих станцій за межами адмінбудівель ради користувач повинен вжити всіх можливих заходів із забезпечення безпечного зберігання та використання ПК, інформації та програмного забезпечення (ПЗ), що на ньому знаходяться.

На робочих станціях, серверному та іншому цифровому обладнанні дозволено використання тільки ліцензійного програмного забезпечення та/або спеціального програмного забезпечення, яке надається авторизованим виробником разом з апаратним забезпеченням.

ПК без нагляду – робочі станції, які залишаються без нагляду повинні бути заблоковані користувачем при виході з робочої зони (робочого місця). Це правило нагадується усім працівникам

під час навчань з інформаційної безпеки. Також на робочих станціях повинно застосовуватись налаштування автоматичного блокування екрана після десяти (10) хвилин бездіяльності. Працівникам заборонено відключати чи змінювати це налаштування без відповідного дозволу відповідального за організацію та забезпечення захисту інформації.

Робочі станції, ноутбуки, телефонні апарати інше цифрове обладнання, яке знаходиться в зоні дозволеної для знаходження відвідувачів, повинні бути облаштовані спеціальними замками та дротом прикріплення для фіксації та унеможливлення їх виносу з місця розташування.

Домашнє використання ПК. Дозволяється підключати до локальної мережі адмінбудівель міської ради тільки таке комп'ютерне обладнання та програмне забезпечення, яке дозволено використовувати. На ПК, що дистанційно підключається до локальних мереж адмінбудівель ради може бути встановлено лише програмне забезпечення, схвалене для використання. Персональні комп'ютери, що надаються для дистанційної роботи, повинні використовуватися виключно в службових цілях. Персонал і підрядники повинні бути ознайомлені і розуміти перелік заборонених видів діяльності, який викладений у п.2.2. нижче. Самовільне переналаштування або зміни конфігурації не допускаються на комп'ютерах, що використовуються для дистанційної роботи персоналом.

Збереження права власності - Усі програмні засоби та документація, що встановлюються на робочих станціях або надаються працівникам чи підрядникам для забезпечення діяльності міської ради, є власністю ради, якщо інше не передбачено умовами відповідного договору. Право власності на програмні засоби зберігається у разі їх офіційного обліку та затвердження відповідним актом (наприклад, актом модернізації автоматизованого робочого місця (АРМ)), у якому зазначається перелік встановленого програмного забезпечення разом із підтвердженням ліцензійних прав. У разі використання на робочих станціях програмного забезпечення з відкритим вихідним кодом або програм, придбаних за кошти працівників, таке ПЗ не вважається власністю міської ради, якщо не оформлено відповідним актом передачі чи договором щодо прав користування.

## 2.2. Заборонена діяльність

Працівникам забороняється здійснювати наступні дії. Перелік не є вичерпним. На інші заборонені види діяльності є посилання в інших місцях цього документа.

- Дії що призводять до збою інформаційної системи. Навмисні дії що призводять до збою інформаційної системи категорично заборонені. Користувачі можуть не усвідомлювати, що вони спричинили збій системи, але якщо буде виявлено, що збій стався в результаті дії користувача, повторні дії користувача, що призводять до збою інформаційної системи можуть розглядатися як навмисний вчинок.

- Спроба несанкціонованого доступу до інформаційного ресурсу або спроба обійти функцію безпеки. Це включає в себе запуск програм для злому паролів або програм для сканування локальної мережі з метою виявлення вразливостей, а також спроби обійти заборону на доступ до інформаційних ресурсів.

- Завантаження або спроба завантаження комп'ютерних вірусів, троянів, шпигунських програм або інших видів шкідливого програмного забезпечення в інформаційну систему. Винятком може бути перевірка стійкості системи уповноваженим персоналом або представниками третьої сторони, що авторизовано перевіряє систему управління інформаційною безпекою.

- Несанкціонований перегляд інформації. Умисний, несанкціонований доступ або перегляд інформації, до якої не надавалися права на доступ чи перегляд відповідно до правила «надання мінімально необхідного доступу» для виконання службових завдань. Цілеспрямована спроба перегляду або доступу до інформації, до якої не було надано доступу за визначеною в політиках інформаційної безпеки процедурою, суворо заборонено.

- Використання особистого або недозволеного програмного забезпечення на робочих станціях. Використання особистого або недозволеного програмного забезпечення на робочих станціях ради заборонено. Все програмне забезпечення, встановлене на робочих станціях, має бути затверджене та дозволене до використання (Додаток 1).

- Використання неліцензійного програмного забезпечення. Все програмне забезпечення, яке встановлене на робочих станціях повинно бути ліцензійним та/або дозволеним до використання.

- Використовувати дозволене програмне забезпечення не належним чином. Порушувати або намагатися порушити умови використання або ліцензійну угоду будь-якого програмного продукту, що дозволено до використання на робочих станціях, суворо заборонено.

- Використовувати інформаційні системи неналежним чином. Брати участь у будь-якій діяльності з будь-якою метою, яка є незаконною або суперечить чинній політиці інформаційної безпеки, суворо заборонено.

### 2.3. Користування Інтернетом та електронною поштою

Електронні засоби комунікації та Інтернет є дієвими інструментами підвищення продуктивності, Ділове використання електронних комунікацій заохочується. Однак усі системи електронного зв'язку та всі повідомлення, що генеруються на обладнанні, що належить виконавчому комітету Миргородської міської ради, або обробляються на пристроях, що належать раді, вважаються власністю виконавчого комітету Миргородської міської ради, а не власністю окремих користувачів. Отже, ця політика поширюється на весь персонал і підрядників (третю сторону) та охоплює всі електронні комунікації, включаючи, але не обмежуючись ними, телефони, електронну пошту, голосову пошту, обмін миттєвими повідомленнями, Інтернет, факс, персональні комп'ютери та сервери.

Надані працівникам інформаційні ресурси, такі як робочі станції або ноутбуки, комп'ютерні системи, мережі, електронна пошта, програмне забезпечення, а також доступ до Інтернет, призначені для використання в ділових цілях. Однак особисте використання допустимо до тих пір, поки це:

- не відволікає від виконання роботи або функціональних обов'язків;
- не зменшує продуктивність працівників;
- не перешкоджає діяльності ради;
- не порушує нічого з наступного:

1) незаконна діяльність - використання інформаційних ресурсів виконавчого комітету Миргородської міської ради для досягнення незаконних цілей або для здійснення правопорушень, суворо заборонено. Порушення авторських прав – це включає скачування, тиражування та використання піратського програмного забезпечення, музики, книг, відео та аудіо файлів, а також незаконне дублювання та/або розповсюдження інформації та іншої інтелектуальної власності, яка перебуває під авторським правом;

2) комерційне використання – використання інформаційних ресурсів виконавчого комітету Миргородської міської ради для отримання особистої вигоди суворо заборонено;

3) політична діяльність – вся політична діяльність суворо заборонена в приміщеннях та з використанням інформаційних ресурсів виконавчого комітету Миргородської міської ради. ОМС заохочує своїх працівників голосувати та активно брати участь у виборчому процесі, але ці заходи не повинні виконуватися з використанням активів та ресурсів виконавчого комітету Миргородської міської ради;

4) переслідування та дискримінація - забороняється використання комп'ютерів, електронної пошти, голосової пошти, обміну миттєвими повідомленнями, текстових повідомлень та Інтернету способами, які є образливими для інших або шкідливими та аморальними. Наприклад, показ або передача зображень, повідомлень і відео сексуального характеру суворо заборонені. Інші приклади неправильного використання включають, але не обмежуються ними - етнічні образи, расові коментарі, або все, що може бути розтлумачено як переслідування, дискримінація, зневажливе ставлення, вираз погроз або прояв неповаги до інших;

5) небажана електронна пошта - усі повідомлення зроблені з використанням ІТ-ресурсів виконавчого комітету Миргородської міської ради повинні бути адресними та доцільними. Розповсюдження «небажаної» пошти, наприклад, листів щастя, реклами або несанкціонованих клопотань, забороняється. Якщо користувачі отримали будь-яке з перерахованого вище повідомлень, необхідно їх видалити та нікому не пересилати.

Установа зберігає за собою право здійснювати моніторинг змісту будь-якого електронного повідомлення та комунікації, що генерується або передається з використанням інформаційних активів виконавчого комітету Миргородської міської ради. Це робиться з метою належного обслуговування та захисту інформаційно- телекомунікаційного обладнання, мереж та ефективного використання наявних ресурсів. Моніторинг може здійснюватися постійно або час від часу. Для цього можуть застосовуватися різні методи моніторингу. Наприклад, коли електронні комунікації можуть контролюватися, включають, але не обмежуються, дослідженнями та тестуваннями спрямованими на оптимізацію ІТ-ресурсів, усунення технічних проблем та виявлення закономірностей зловживань або незаконної діяльності.

Установа залишає за собою право на власний розсуд переглядати файли або електронні повідомлення будь-якого працівника в обсязі, необхідному для забезпечення ефективного використання всіх службових електронних носіїв і засобів комунікації відповідно до всіх чинних законів і нормативних актів, а також цієї Політики інформаційної безпеки.

Доступ в Інтернет надається тільки тим співробітникам, хто його потребує для виконання службових обов'язків. Персонал, що має доступ до Інтернету, не повинен використовувати цей доступ для розваг, прослуховування музики чи радіо, прослуховування онлайн аудіо книг та перегляду фільмів та інших медійних файлів тощо. Забороняється використовувати доступ до Інтернет для особистої комерційної діяльності чи вирішення своїх побутових питань. Треба розуміти, що використання цього ресурсу не цільовим шляхом створює додаткові загрози інформаційної безпеки.

Персонал повинен розуміти, що індивідуальне використання Інтернету контролюється, і якщо виявиться, що співробітник витрачає надмірну кількість часу, витрачає великі обсяги трафіку для особистого чи нецільового користування, або відвідує ресурси, які небезпечні з точки зору забезпечення інформаційної безпеки, то до нього/неї будуть вжиті дисциплінарні заходи.

Ресурси які заборонено відвідувати, такі як ігрові інтернет-сайти, торенти, файлообмінники, порносайти, чати та онлайн програми для обміну музикою, тощо, автоматично блокуються. Перелік заборонених ресурсів постійно контролюється і оновлюється в міру необхідності. Будь-який співробітник, який цілеспрямовано, неодноразово буде намагатися відвідати заборонені ресурси в Інтернет, буде притягнутий до дисциплінарної відповідальності.

Використовуючи електронну пошту потрібно дотримуватись наступних правил безпеки:

➤ двофакторна автентифікація (2FA): обов'язково увімкніть підтвердження входу через SMS або додаток (наприклад, Google Authenticator). Це найкращий захист, навіть якщо пароль дізнаються сторонні;

➤ складний пароль: використовуйте унікальну комбінацію з літер, цифр і символів. Не використовуйте один і той самий пароль для пошти та соцмереж;

➤ обережно з вкладеннями: ніколи не відкривайте файли (особливо з розширеннями .exe, .zip, .pdf, .xls з макросами) від незнайомих відправників. У них може бути вірус;

➤ ігноруйте підозрілі посилання: шахраї часто маскуються під банки або техпідтримку (фішинг). Завжди перевіряйте реальну адресу відправника, перш ніж щось натиснути;

➤ не використовуйте публічний Wi-Fi: якщо потрібно зайти в пошту через відкриту мережу в кафе чи аеропорту, обов'язково вмикайте VPN;

➤ виходьте з акаунта: якщо ви скористалися поштою на чужому комп'ютері, завжди натискайте «Вийти» та не зберігайте пароль у браузері.

В установі здійснюються спеціальні запобіжні заходи для блокування зовнішнього доступу через Інтернет до інформаційних ресурсів міської ради, не призначених для публічного доступу, а також для захисту конфіденційної інформації ради при її передачі через Інтернет.

Відповідальний за інформаційну безпеку контролює виконання заходів із безпечного використання Інтернету, а саме:

- контролює щоб доступ до Інтернет з робочих місць здійснювався через встановлені точки доступу до Інтернет;

- контролює, щоб тільки публічна та відкрита інформація була доступна в Інтернеті;

- контролює, щоб користувачі не мали прав встановлювати або завантажувати будь-яке програмне забезпечення (додатки тощо) з Інтернет. Якщо у користувачів є потреба в додатковому програмному забезпеченні, користувач повинен отримати дозвіл;

- використання мережі на робочому місці для отримання особистого прибутку заборонено;

- конфіденційні або персональні дані, включаючи номери кредитних карток, номери телефонів, паролі для входу в систему та інші дані, які можуть бути використані для доступу до конфіденційної або персональної інформації повинні передаватися через Інтернет у зашифрованому виді;

- використання програмного забезпечення для шифрування та ключів шифрування повинно контролюватися відповідальним за інформаційну безпеку. Самостійне використання шифрувального програмного забезпечення та ключів шифрування, без погодження з відповідальним за інформаційну безпеку, заборонено і може призвести до дисциплінарного покарання.

#### 2.4. Користування зовнішніми CD/DVD/USB-пристроями

Використовуючи зовнішні пристрої необхідно пам'ятати та суворо дотримуватись наступних правил:

- скануйте на віруси: завжди перевіряйте антивірусом будь-який зовнішній носій одразу після підключення, особливо якщо він побував у чужому комп'ютері;
- не використовуйте знайдені пристрої: ніколи не підключайте флешки, які ви знайшли на вулиці чи в офісі. Це поширений метод хакерських атак (так званий "USB dropping");
- використовуйте шифрування: якщо ви зберігаєте на диску конфіденційну інформацію, захистіть її паролем за допомогою вбудованих засобів (наприклад, BitLocker для Windows або 7-Zip);
- розділяйте особисте та робоче: не підключайте домашні флешки до робочих комп'ютерів і навпаки, щоб уникнути перехресного зараження вірусами;
- вимкніть автозапуск: налаштуйте операційну систему так, щоб вона не запускала файли з флешки автоматично при підключенні;
- безпечно вилучення: завжди використовуйте функцію «Безпечно вилучення пристрою», щоб не пошкодити файлову систему та не втратити дані;
- фізичний захист: тримайте носії в сухому місці та захищайте їх від ударів. Для особливо важливих даних використовуйте флешки з апаратним захистом (введення коду на самому корпусі).

#### 2.5. Повідомлення про несправності

Користувач повинні інформувати IT підрозділ про випадки, коли програмне забезпечення робочої станції не функціонує належним чином. Несправне програмне забезпечення становить ризик для інформаційної безпеки. Якщо користувач, або керівник користувача, підозрює зараження робочої станції вірусом, слід негайно вжити наступних заходів:

- припинити використання комп'ютера;
- не запускати на виконання ніяких команд, включаючи команду збереження даних;
- не закривати жодного з вікон або програм комп'ютера;
- не вимикати комп'ютер або периферійний пристрій на самому екрані;
- по можливості фізично відключити комп'ютер від мереж живлення та локальної мережі;
- повідомити про ураження робочої станції IT-підрозділ та відповідального за інформаційну безпеку, вказавши ознаки незвичайної поведінки комп'ютера (блокування екрану, виникнення несподіваного доступ до системного диска, незвичайна реакція на команди тощо) і час, коли це було вперше помічено;
- повідомити про будь-які зміни у використанні апаратного чи програмного забезпечення, які передували несправності;
- не намагатися самостійно видалити підозрілий файл!

Відповідальний за інформаційну безпеку повинен вжити заходи для усунення несправності, а також повідомити вище керівництво про результати цих дій з рекомендаціями щодо подальших кроків для запобігання подібних випадків у майбутньому.

#### 2.6. Повідомлення про інциденти безпеки

Весь персонал, який є користувачами інформаційних ресурсів або підрядники, які мають доступ до цифрових активів виконавчого комітету Миргородської міської ради зобов'язані повідомляти відповідального з ІБ про виявлені інциденти інформаційної безпеки. Користувач - це будь-яка особа, уповноважена на доступ до інформаційного ресурсу ради. Користувачі несуть відповідальність за повсякденну практичну безпеку ресурсу, яким вони користуються. Користувачі повинні повідомляти про всі інциденти безпеки або порушення політики безпеки негайно своєму безпосередньому керівнику або відповідальному з інформаційної безпеки.

Реагування на повідомлення про інциденти інформаційної безпеки повинно бути якомога швидким. Необхідно негайно вжити заходи відповідно до Плану реагування на інцидент інформаційної безпеки. Кожен інцидент повинен бути проаналізованим, щоб визначити, чи потрібно внесення необхідних змін в існуючу систему управління інформаційною безпекою виконавчого комітету Миргородської міської ради. Усі виявлені інциденти реєструються в журналі інцидентів інформаційної безпеки (Додаток 2). Обов'язком відповідального за ІБ є організація та проведення навчання, щодо будь-яких змін у плані реагування на інциденти, які були зроблені в результаті розслідування інциденту.

Внутрішні порушення інформаційної безпеки повинні оперативно розслідуватися. У разі підозри на порушення законодавства, відповідальний з ІБ повинен звернутися до правоохоронних органів.

### **2.7 Передача конфіденційної інформації**

Передача конфіденційної інформації може здійснюватися за допомогою засобів електронного зв'язку, на цифрових носіях чи у паперовому виді. Конфіденційна інформація передається від однієї особи іншій під час ведення службових справ. Особа, яка отримала конфіденційну інформацію повинна забезпечити її зберігання відповідно до умов, встановлених особою, що надала таку інформацію.

### **2.8. Передача даних та програмного забезпечення**

Власне програмне забезпечення, яке не дозволене до використання в закладі, не може використовуватися на робочих станціях чи комп'ютерах або в локальній мережі виконавчого комітету Миргородської міської ради. Якщо існує потреба в конкретному програмному забезпеченні, потрібно надати запит на дозвіл своєму безпосередньому керівнику. Користувачі не повинні використовувати програмне забезпечення, що встановлене на робочих станціях, або на особистих комп'ютерах чи комп'ютерному обладнанні при дистанційній роботі без відповідного дозволу.

Дані, що є власністю міської ради включаючи інформацію про працівників, інформацію про ІТ-системи, фінансову інформацію або дані про людські ресурси, не повинні розміщуватися на будь-якому комп'ютері, який не є власністю ради, без письмової згоди відповідного керівника. У випадку, якщо відповідний керівник отримує від працівників запит на переміщення даних з робочої станції на особистий ПК, керівник повинен визначитися чи є в цьому службова потреба та у разі прийняття рішення на дозвіл переміщення, повідомити відповідального з інформаційної безпеки про таку передачу даних.

Треба розуміти, що установа обмежена у можливостях захисту даних на персональних ПК тому дозвіл на переміщення треба надавати у разі гострої службової необхідності. Установа не може бути впевнена у засобах, які можуть бути застосовані для захисту конфіденційної чи чутливої інформації на персональних ПК, звідси необхідність цього обмеження.

### **2.9. Шифрування електронної пошти та даних**

Для забезпечення конфіденційності та захисту конфіденційної інформації при передачі в мережі Інтернет дозволяється використання відповідного програмного забезпечення (наприклад програми 7-Zip), яке дозволяє працівникам обмінюватися електронною поштою з віддаленими користувачами, які теж мають відповідне програмне забезпечення для шифрування/дешифрування. Обидва користувачі обмінюються таємними паролями (у випадку використання 7-Zip) або відкритими ключами, які можуть бути використані для дешифрування повідомлення. Співробітник, який бажає використати відповідне програмне забезпечення повинен звернутися до відповідального за ІБ для отримання дозволу на використання відповідного програмного забезпечення.

При передачі конфіденційної інформації електронною поштою та розумінні, що є ризик потрапляння такої інформації до сторонніх осіб чи отримання доступу до неї сторонніми особами необхідно застосовувати програмне забезпечення шифрування/дешифрування (наприклад 7-Zip).

## **3. УПРАВЛІННЯ ДОСТУПОМ**

### **3.1. Встановлення паролів**

Ідентифікатори користувачів і паролі потрібні для того, щоб отримати доступ до мереж та робочих станцій. До всіх паролів застосовується встановлена цим документом Парольна політика, для забезпечення стійкості паролів. Це означає, що всі паролі повинні відповідати вимогам, які призначені для того, щоб пароль було важко підібрати чи зламати. Користувачі зобов'язані створювати та користуватися паролями, щоб отримати доступ до відповідних мереж, ІТ-ресурсів чи робочої станції. При призначенні паролю користувачеві буде автоматично запропоновано вручну призначити пароль, відповідно до таких вимог:

**Довжина пароля** – пароль повинен складатися з мінімум восьми (8) символів.

**Вимоги до складу** - пароль повинен містити комбінацію символів латинського алфавіту верхнього та нижнього регістру, числових символів та спеціальних символів.

**Частота зміни** – Пароль повинен бути змінений кожні 90 днів. Скомпрометований пароль повинен бути змінений негайно.

**Повторне використання** - Попередні три (3) паролі не можуть бути використані повторно.

**Обмеження на обмін паролями** - Паролі не повинні передаватися іншим працівникам, записуватися на папері або зберігатися на робочій станції і повинні зберігатися у таємниці.

**Обмеження на відображення та зберігання паролів** - Паролі маскуються на екрані робочої станції при введенні, не друкуються і не включаються до електронних журналів чи звітів. Паролі зберігаються у зашифрованому виді.

### 3.2. Угода про конфіденційність

Користувачі інформаційних ресурсів виконавчого комітету Миргородської міської ради при працевлаштуванні підписують угоду про конфіденційність. Угода повинна містити наступне твердження:

*Я розумію, що будь-яке несанкціоноване використання або розголошення конфіденційної інформації, може призвести до покарання, відповідно до чинного законодавства та політики інформаційної безпеки.*

Тимчасово влаштовані працівники та підрядники, які не підписували угоди про конфіденційність, підписують такий документ при отриманні доступу до інформаційних ресурсів міської ради.

Угода про конфіденційність переглядається, коли відбуваються зміни умов трудової діяльності, зокрема при звільненні працівника.

## 4. ПІДКЛЮЧЕННЯ ДО МЕРЕЖІ

### 4.1. З'єднання та підключення

Доступ до інформаційних ресурсів виконавчого комітету Миргородської міської ради через маршрутизатори, інші комунікаційні пристрої або відповідне програмне забезпечення підлягає авторизації та автентифікації системою контролю доступу. Зовнішній виклик чи комутація на внутрішні (кінцеві пристрої) без проходження через систему контролю доступу заборонений.

Системи, що дозволяють проходження зовнішнього виклику на кінцевий пристрій, в тому числі сервер повинні гарантувати додаткову безпеку на рівні операційної системи та додатків. Такі системи повинні також мати можливість контролювати рівень активності, щоб гарантувати, що використання кінцевих пристроїв відбувається належним чином та з виконанням заходів безпеки.

Права доступу до з'єднання через комутатори надаються тільки на вимогу керівника відділу з поданням Форми доступу (Додаток 3) та затверджуються відповідальним з ІБ.

Підключення до зовнішніх мереж відбувається через інтернет-провайдера. Якщо користувач має конкретну потребу зв'язатися із зовнішнім комп'ютером або мережею через прямий канал зв'язку він повинен отримати дозвіл від відповідального з ІБ. При прийнятті позитивного рішення відповідальний з інформаційної безпеки повинен вжити необхідних заходів із забезпечення належного рівня безпеки нового каналу зв'язку.

### 4.2. Телекомунікаційне обладнання

До телекомунікаційного обладнання та засобів відноситься наступне:

- комутатори, маршрутизатори, точки доступу та подібне обладнання;
- мережеві лінії (оптичні, дротові);
- телефонні лінії та обладнання;
- телефонні навушники та гарнітура;
- телефони типу програмного забезпечення, встановлені на робочих станціях;
- службові мобільні телефони;
- програмне забезпечення для маршрутизації викликів;
- обладнання для адміністрування телефонної системи.

Цей перелік не є вичерпним.

### 4.3. Постійні з'єднання

Забезпечення безпеки телекомунікаційних з'єднань є дуже важливим завданням. Інформаційна безпека міської ради може бути поставлена під загрозу, якщо не забезпечити безпечне користування засобами зв'язку. Необхідно забезпечити аналіз ризиків при підключенні до зовнішніх мереж та

регулярно аналізувати ризики постійно діючих каналів з'єднання. Аналіз ризиків повинен враховувати тип необхідного доступу, цінність інформації що передається, заходи безпеки, що застосовуються третьою стороною, а також наслідки для системи управління безпекою. Відповідальний за інформаційну безпеку повинен бути залучені до процесів проєктування та затвердження каналів підключення до зовнішніх мереж, а також укладення договорів з третьою стороною на отримання послуг з телекомунікаційного забезпечення.

#### 4.4. Договір на телекомунікаційні послуги

При укладанні договору на отримання телекомунікаційних послуг установою необхідно враховувати наступні вимоги до постачальника таких послуг:

- відповідні розділи політики інформаційної безпеки надавача послуг були переглянуті та приведені у відповідність з вимогами політики інформаційної безпеки;
- відповідні вимоги враховані та застосовуються;
- проведена оцінка ризиків пов'язаних з виконанням додаткових зобов'язань надавача послуг;
- включене право на аудит виконання договірних зобов'язань;
- домовленість стосовно повідомлення про інциденти інформаційної безпеки включенні в угоду;
- наданий опис кожної послуги, яка буде доступна;
- доступ до ресурсів міської ради надавачем послуг повинен бути лише на мінімально необхідному рівні, достатньому для виконання договірних зобов'язань;
- детальний список користувачів з боку надавача послуг, які будуть мати доступ до мережі міської ради, повинен бути доступний для аудиту;
- дата і час, коли послуга повинна бути доступна, завчасно узгоджені;
- процедури щодо захисту інформаційних ресурсів узгоджені заздалегідь, а спосіб аудиту затверджений обома сторонами;
- спосіб моніторингу і припинення доступу користувачів визначений;
- обмеження на копіювання та розкриття інформації включені;
- обов'язки щодо встановлення та технічного обслуговування апаратного та програмного забезпечення зрозумілі та заздалегідь узгоджені;
- заходи щодо забезпечення повернення або знищення програмного забезпечення та інформації після закінчення дії договору визначені та прописані;
- заходи фізичного захисту, при необхідності, також включенні в угоду;
- спосіб надання доступу та авторизація користувачів, повинен бути встановлений до того, як користувачам буде наданий доступ;
- створені механізми для забезпечення дотримання заходів безпеки сторонами угоди;
- детальний перелік заходів безпеки, які будуть вжиті сторонами угоди, повинен бути розглянутий та погоджений до укладення угоди.

#### 4.5. Брандмауер

Налаштування брандмауера повинно контролюватися відповідальним з ІБ. Якщо брандмауер знаходиться та налаштовується стороною, яка надає ІТ-послуги управлінню, то ця сторона повинна надати повну інформацію про актуальні налаштування брандмауера відповідальному за інформаційну безпеку та активно співпрацювати з ним/нею у питаннях подальшого його використання та змін налаштувань.

### 5. АНТИВІРУСНИЙ ЗАХИСТ

#### 5.1. Встановлення та оновлення антивірусного ПЗ

Антивірусне програмне забезпечення встановлюється на всіх робочих станціях, кінцевому обладнанні і серверах та періодично (щодня) оновлюється. За своєчасне оновлення антивірусного програмного забезпечення відповідає ІТ-підрозділ (системний адміністратор).

Конфігурації - антивірусне програмне забезпечення, яке на даний час використовується, це ESET. Оновлення відбувається щодня автоматично.

Конфігурація віддаленого розгортання - за допомогою автоматизованої процедури встановлення та оновлення антивірусне ПЗ може бути встановлене та оновлене на окремих віддалених робочих станціях та серверному обладнанні за потреби.

Моніторинг/Звітність – в установі ведеться контроль оновлення та застосування антивірусного

програмного забезпечення. IT-підрозділ (системний адміністратор) несе відповідальність за надання звітів про перевірку спрацювання антивірусного програмного забезпечення при інцидентах інформаційної безпеки.

## **5.2. Перевірка нового ПЗ**

На внутрішніх комп'ютерах і мережах використовується лише дозволене до використання програмне забезпечення. Встановлення нового програмного забезпечення потребує отримання дозволу відповідального з інформаційної безпеки. Перелік дозволеного до використання програмного забезпечення наведений у Додатку 2. Перед встановленням нове програмне забезпечення проходить перевірку IT-підрозділом з метою забезпечення сумісності зі встановленим на даний момент програмним забезпеченням і конфігурацією мережі. Крім того, IT- підрозділ повинен перевірити нове ПЗ за допомогою наявного антивірусного програмного забезпечення на наявність вірусів та інших шкідливих програм перед установкою. Це стосується як програмного забезпечення, що закуповується так і умовно-безкоштовного програмного забезпечення.

Хоча умовно-безкоштовне програмне забезпечення може бути корисним, використання такого програмного забезпечення має бути попередньо схвалено відповідальним з інформаційної безпеки. Оскільки програмне забезпечення часто завантажуються з Інтернет (загальнодоступного джерела) і може мати віруси та інше шкідливе програмне забезпечення, перед його встановленням на комп'ютерах необхідно вжити спеціальних запобіжних заходів. Ці запобіжні заходи включають визначення того, що програмне забезпечення є сумісним з існуючим ПЗ, не перешкоджає або не пошкоджує апаратне забезпечення, програмне забезпечення або інформацію, а також що програмне забезпечення не містить вірусів та інших шкідливих програм.

Усі файли і програми, які були передані в електронному вигляді на комп'ютери або мережу з іншого місця, повинні бути перевірені на віруси відразу після отримання. Перевірка та сканування на віруси здійснюється автоматично встановленим антивірусним ПЗ або в ручному режимі. Якщо отримані файли/програми викликають підозру (отримані з невідомих джерел, мають невідповідне чи небезпечне розширення та подібне) необхідно сповістити про це IT-підрозділ для проведення додаткового аналізу цих файлів.

Кожен CD/DVD/USB-пристрій є потенційним джерелом комп'ютерного вірусу. Тому такі зовнішні носії інформації повинні бути проскановані на наявність вірусів та іншого шкідливого програмного забезпечення, перш ніж інформація з них буде скопійована на комп'ютери.

Забороняється завантажувати комп'ютери з CD/DVD/USB-пристроєм, отриманого із зовнішнього джерела. Користувачі завжди повинні видаляти будь-які зовнішні носії з комп'ютера, коли він не використовується. Це робиться для того, щоб CD/DVD/USB -пристрій не знаходилися в комп'ютері під час його включення.

## **5.3. Збереження прав власності**

Усі програмні продукти та документація, що надаються працівникам або підрядникам є власністю виконавчого комітету Миргородської міської ради, якщо на них не поширюється дія іншого договору. Програмні засоби, застосунки або документація які розробляються за замовленням є також її власністю. Розробники таких програмних продуктів та документації повинні підписати заяву, в якій визнається право власності на відповідний програмний продукт та документацію. Програмне забезпечення, придбане працівником за власний рахунок, залишається власністю працівника, який придбав це програмне забезпечення.

# **6. КРИПТОГРАФІЧНИЙ ЗАХИСТ**

## **6.1. Визначення**

Криптографічний захист інформації за допомогою шифрування даних є найефективнішим способом забезпечення безпеки даних виконавчого комітету Миргородської міської ради. Шифрування це процес перетворення інформації, використовуючи криптографічний алгоритм, щоб зробити її нечитабельною для будь-кого, крім тих, хто має авторизовану «потребу знати». Щоб отримати доступ до зашифрованої інформації, необхідно мати доступ до секретного ключа або паролю, що дозволяє його розшифрувати. В установі використовуються наступні засоби криптографічного захисту: інфраструктура відкритих ключів з електронним цифровим підписом; програма-архіватор 7-Zip; BitLocker для Windows; захищений веб-інтерфейс SSL.

## **6.2. Ключі шифрування**

Ключ шифрування визначає особливе перетворення простого тексту у зашифрований, або навпаки під час дешифрування (розшифрування). Якщо це обґрунтовано аналізом ризиків інформаційної безпеки, конфіденційні дані та файли, що містять конфіденційну інформацію, повинні бути зашифровані перед передачею через мережу загального користування чи Інтернет. Коли зашифровані дані передаються між установою та сторонньою організацією необхідно розробити та запровадити взаємну процедуру обміну та безпечного управління ключами. У разі виникнення інциденту, пов'язаного з криптографічним захистом інформації, його вирішенням повинен займатися відповідальний з інформаційної безпеки. Установа може використовувати декілька методів безпечної передачі даних за допомогою криптографічного захисту.

## **6.3. Використання інфраструктури відкритих ключів**

Користувач, який має потребу у безпечній передачі інформації електронною поштою конкретному ідентифікованому зовнішньому користувачеві, може скористатися інфраструктурою відкритих ключів та електронним цифровим підписом (ЕЦП). Порядок використання ЕЦП у установі повинно бути погоджено з керівником чи відповідальним за інформаційну безпеку.

## **6.4. Використання 7-Zip**

Це програмне забезпечення дозволяє працівникам обмінюватися електронною поштою з віддаленими користувачами, які мають відповідне програмне забезпечення для шифрування та дешифрування. Обидва користувачі обмінюються паролем, який використовується як для шифрування, так і для дешифрування/розшифрування кожного повідомлення. Пароль передається отримувачу альтернативним засобом зв'язку, таким як смс, месенджер або телефоном.

## **6.5. Веб-інтерфейс рівня захищених сокетів (SSL)**

Для передачі конфіденційної інформації через веб-інтерфейсі використовується веб-інтерфейс захисту SSL. SSL (англ. Secure Sockets Layer) — криптографічний протокол, який забезпечує встановлення безпечного з'єднання між клієнтом і веб-сервером. Протокол забезпечує конфіденційність обміну даними між клієнтом і сервером, що використовують TCP/IP. Користувач через веб-інтерфейс захисту SSL передає/отримує конфіденційну інформацію через веб-сторінку в Інтернеті при наданні/отриманні послуг онлайн. Порядок використання веб-інтерфейсу захисту SSL погоджується з відповідальним з інформаційної безпеки.

# **7. ФІЗИЧНА БЕЗПЕКА**

Забезпечення фізичної безпеки працівникам полягає у створенні безпечних умов на робочому місці та одночасним забезпеченням безпечного зберігання активів виконавчого комітету Миргородської міської ради. Адмінбудівля (комплекс будівель) є дещо унікальним місцем з точки зору прав власності на будівлю або умов договору оренди, території навколо, шляхів під'їзду/виїзду, зовнішнього огороження, входів у приміщення, вимог до пожежної безпеки, систем електроживлення, відеоспостереження, забезпечення безпечного використання цифрових активів та контролю серверної кімнати. Необхідно постійно покращувати та модернізувати систему забезпечення фізичної безпеки для підвищення захисту своїх активів та інформації.

Адмінбудівля обладнана системою резервного живлення, а саме генератором.

# **8. ДИСТАНЦІЙНА РОБОТА**

В установі дозволяється та використовується дистанційна робота працівників при певних, визначених керівництвом обставинах. Вимоги, щодо організації дистанційної роботи застосовуються до всіх працівників і підрядників, які працюють поза межами будівлі (комплексу будівель) виконавчого комітету Миргородської міської ради.

Хоча дистанційна робота може бути перевагою як для користувачів, так і для організації в цілому, вона представляє нові ризики інформаційної безпеки. Персонал, що працює дистанційно повинен бути захищеним від небезпеки атак шкідливим програмним забезпеченням та несанкціонованого витоку даних з пристроїв, що знаходяться за межами периметру безпеки.

## **8.1. Загальні вимоги**

Користувачі, що працюють віддалено, зобов'язані дотримуватися всіх правил, які встановлені

для працівників та підрядників, а саме:

**Потрібно знати:** користувачі, що працюють віддалено, мають доступ тільки до тих ресурсів та інформації, які потрібні для виконання функціональних завдань.

**Використання пароля:** користувачі, що працюють віддалено, повинні дотримуватись вимог щодо встановлення та зміни паролів. Окрім того, вони не розголошують свій пароль і не залишають записів щодо паролю там, де такий запис може побачити член сім'ї або стороння особа.

**Навчання:** персонал, який працює віддалено, повинен проходити ті самі навчання з інформаційної безпеки, що і персонал що працює на робочих місцях.

**Специфічні вимоги:** до працівників, що працюють віддалено, можуть бути застосовані додаткові вимоги, які пов'язані зі специфікою виконання функціональних завдань дистанційно.

## 8.2. Необхідне обладнання

Працівники, допущені до дистанційної роботи, повинні розуміти, що установа не надає все обладнання, необхідне для забезпечення належного захисту інформації, до якої працівник має доступ

**Працівник повинен забезпечити самостійно:**

- о робочий комп'ютер (ноутбук) зі встановленим антивірусним ПЗ та програмним забезпеченням шифрування даних;
- о зовнішній носій для резервного копіювання;
- о широкосмуговий канал доступу до Інтернет;
- о подрібнювач паперу або можливість іншим способом знищувати паперові носії;
- о відокремлене від членів родини робоче місце;
- о шафа, що зачиняється або сейф для захисту та зберігання робочого комп'ютера та робочих документів.

## 8.3. Захист апаратного забезпечення

**Захист від вірусів:** користувач, що працює дистанційно, повинен постійно використовувати та оновлювати захист комп'ютера від вірусів та іншого шкідливого програмного забезпечення. Антивірусне програмне забезпечення встановлене на комп'ютерах і налаштоване на періодичне оновлення. Заборонено працювати без оновленого антивірусного програмного забезпечення.

**Використання VPN та брандмауера:** при дистанційному підключенні повинен використовуватись канал зв'язку, який вимагає використання VPN та брандмауера. При відключенні VPN та/або брандмауера дистанційну роботу потрібно зупинити.

**Шафа або сейф:** використовуйте шафу, що замикається або сейф для безпечного зберігання комп'ютеру та інших пристроїв наданих установою для дистанційної роботи.

**Захист ПК:** персональний комп'ютер, що використовується для дистанційної роботи, повинен бути облаштований спеціальним замком для захисту від крадіжки.

**Блокування екранів:** незалежно від місця розташування завжди блокуйте екран перш ніж відійти від робочої станції. Дані на екрані можуть містити конфіденційну інформацію. Переконайтеся, що функцію автоматичного блокування настроєно на автоматичне ввімкнення після 10 хвилин бездіяльності.

## 8.4. Безпека даних

**Резервне копіювання даних:** встановлена процедура резервного копіювання, яка шифрує дані, та переміщує їх на зовнішній носій. Для резервного копіювання використовується тільки встановлена процедура. Створювати самостійно інші процедури резервного копіювання даних заборонено. Якщо неможливо дотримуватись встановленої процедури резервного копіювання: не має відповідного програмного забезпечення та/або зовнішнього носія – резервне копіювання заборонено. Дозволено використовувати наявні засоби шифрування (BitLocker для Windows та архіватор-шифрувальник 7-Zip) та доступний зовнішній носій. Причому, безпечному зберігання зовнішнього носія з резервною копією даних треба приділити значну увагу.

**Передача даних:** передача даних до вимагає використання затвердженого VPN-з'єднання для забезпечення конфіденційності та цілісності даних, що передаються. Не дозволено обходити встановлену процедуру, а також створювати власний метод передачі даних.

**Доступ до зовнішніх систем (хмар):** якщо є потреба у доступі до зовнішньої ІТ-системи, необхідно зв'язатися зі своїм безпосереднім керівником або відповідальним за інформаційну

безпеку. Вони визначають безпечний метод доступу до потрібної зовнішньої системи.

Електронна пошта: не дозволено передавати будь-яку конфіденційну інформацію та персональні дані електронною поштою, якщо вона не зашифрована. При гострій необхідності треба звернутися до свого безпосереднього керівника або відповідального за інформаційну безпеку. Вони визначають безпечний метод передачі конфіденційної інформації та персональних даних електронною поштою.

Підключення через публічний WiFi: необхідно дотримуватися надзвичайної обережності при підключенні до IT-систем через публічну точку доступу до Інтернет. Хоча установа застосовує системи безпеки для захисту даних проте установа не може забезпечити захист даних у мережевому обладнанні, що знаходиться поза межами адмінбудівлі.

Захистити дані, якими ви володієте: потрібно отримувати доступ лише до тієї інформації, яка потрібна для виконання робочого завдання. Регулярно переглядайте дані, які ви зберегли, щоб переконатися, що масив даних, який зберігається знаходиться на мінімально необхідному рівні, а застарілі дані та версії файлів видалені. Зберігайте електронні дані тільки в зашифрованому виді. Якщо на ноутбуку не встановлено відповідне ПЗ для шифрування треба звернутися до IT-підрозділу.

Друковані звіти або робочі документи: ніколи не залишайте паперові документи на робочому столі коли ви залишаєте робоче місце. Всі паперові документи повинні зберігатися у замкненій шафі або сейфі.

Введення даних у відкритому місці: не виконуйте робочі завдання, які вимагають використання конфіденційної інформації або персональних даних у громадських місцях.

Надсилання даних за межі адмінбудівлі: вся передача даних за межі адмінбудівлі повинна бути пов'язана з виконанням вимог договорів та дотримуватися вимог угод про конфіденційність і нерозголошення конфіденційної інформації. При необхідності передачі інформації стороннім організаціям з якими не укладено договорів та угод на обмін інформацією необхідно отримати письмову згоду безпосереднього керівника.

## **8.5. Утилізація паперових та зовнішніх носіїв**

Паперові документи: Всі паперові документи, які містять конфіденційну інформацію, перед утилізацією потрібно подрібнити. Заборонено викидання не подрібнених паперових документів. Персонал, який працює дистанційно, повинен мати або подрібнювач паперу або можливість спалювання паперових документів.

Зовнішні носії: Всі зовнішні носії, надані для забезпечення дистанційної, роботи повинні бути повернуті для утилізації.

## **9. ПОЛІТИКА ЧИСТОГО СТОЛУ/ЕКРАНУ**

Одним із засобів контролю за забезпечення інформаційної безпеки є політика чистого столу та чистого екрану, яка знижує ризик несанкціонованого доступу, втрату та пошкодження інформації протягом робочого часу та після його закінчення. Політика чистого столу та чистого екрану визначає методи, пов'язані із забезпеченням того, щоб конфіденційна інформація, як у цифровому, так і у паперовому/фізичному форматі, та активи (наприклад, робочі станції, ноутбуки, стаціонарні телефонні апарати, смартфони, цифрове обладнання та інші) не залишаються без захисту, коли вони не використовуються, чи коли персонал залишає свої робочі місця на короткий час або наприкінці дня. Дотримання політики чистого столу/екрану всього без винятку працівників дозволить суттєво убезпечити виконавчий комітет Миргородської міської ради від витоку конфіденційної інформації.

Метою впровадження політики чистого столу та чистого екрану у виконавчому комітеті Миргородської міської ради є:

- запобігання витоку/втраті конфіденційних даних;
- дотримання правил кібергігієни та розвитку кіберкультури щодо безпечного та належного поводження з конфіденційною інформацією та її носіями.

### **Відповідальність**

Вимоги цієї політики поширюються на весь персонал міської ради. Усі працівники мають бути ознайомлені із її вимогами. До будь-якого працівника, визнаного винним у порушенні цієї політики, може бути застосована дисциплінарна практика.

## **Вимоги**

Увесь персонал повинен дотримуватись наступних правил:

- зберігати власні паролі в таємниці, не розголошувати та нікому не повідомляти їх;
- закривати активні сеанси після завершення роботи, якщо їх не можна захистити відповідним блокуючим механізмом, наприклад блокуванням екрану;
- встановити час автоматичного блокування екрану робочої станції 10 хвилин;
- по завершенні сеансу виходити із ІТ-систем та баз даних, до яких протягом сеансу був отриманий доступ (серверів, додатків, VPN – каналів тощо);
- забороняється вести запис паролів (наприклад, на папері, у програмному файлі або в кишеньковому пристрої), за винятком тих випадків, коли запис може зберігатися безпечно, а метод зберігання був затверджений відповідальним за ІБ;
- матеріальні носії конфіденційної інформації повинні замикатися в сейфі або шафі після завершення роботи з ними;
- робочі станції, комп'ютери та засоби зв'язку повинні бути залишені у стані виконаного виходу із системи/вимкнені коли вони перебувають без нагляду;
- цифрове обладнання, що не використовується повинно бути вимкнено або переведене у безпечний режим;
- документи, які містять конфіденційну інформацію, повинні витягатися виконавцем з принтерів негайно;
- наприкінці робочого дня/зміни увесь персонал повинен упорядковувати своє робоче місце та прибрати всі робочі документи в сейф або шафу, що замикається;
- для утилізації конфіденційних документів слід використовувати знищувачі/подрібнювачі паперу;
- після закінчення робочого дня та у разі тривалої відсутності на робочому місці необхідно замикати на замок усі шафи та сейфи де зберігається конфіденційна інформація та робочі документи.

## **10. ОБІЗНАНІСТЬ ТА НАВЧАННЯ З ПИТАНЬ БЕЗПЕКИ**

Для підвищення обізнаності стосовно питань інформаційної безпеки весь персонал, включаючи керівництво, повинен регулярно проходити відповідні навчання. Навчання з ІБ для всіх працівників проводиться раз на шість місяців, або позапланово при необхідності.

### **Навчальна програма з інформаційної безпеки**

Відповідальний за інформаційну безпеку організовує та проводить навчання з інформаційної безпеки. Він/вона здійснює первинний інструктаж для нових працівників, щорічний інструктажі для всіх працівників, а також планові заняття стосовно Політики інформаційної безпеки та актуальних загроз. Для проведення навчань відповідальний з ІБ може залучати інших працівників та сторонніх експертів, в тому числі виробників ІТ-систем та розробників програмного забезпечення. Відвідування та/або участь у такому навчанні є обов'язковим для всіх працівників.

Відповідальний з ІБ, при необхідності, може організовувати позапланові навчання при змінах у апаратному або програмному забезпеченні, збільшенні загроз, внесенні змін у політику інформаційної безпеки, за результатами аудиту, тощо.

### **Пам'ятка з інформаційної безпеки**

Відповідальний за ІБ розробляє пам'ятку з інформаційної безпеки, до якої включає правила кібергігієни та правила чистого столу. Пам'ятка містить актуальну інформацію стосовно безпеки паролів, шкідливого програмного забезпечення, ідентифікації та реагування на інциденти, а також контролю доступу. Відповідальний за ІБ забезпечує доведення пам'ятки з інформаційної безпеки до всіх працівників. Окрім того він/вона може поширювати спеціальні повідомлення до працівників стосовно нових загроз, небезпеки, вразливостей та необхідних заходах інформаційної безпеки.

### **Захист від шкідливого програмного забезпечення**

У рамках вищезазначеної навчальної програми з безпеки відповідальний за ІБ проводить навчання щодо запобігання ураження та протидії шкідливому програмному забезпеченню. Таке навчання повинно включати в себе наступне:

- вказівки щодо поведінки з підозрілим вкладенням електронної пошти, електронними листами від незнайомих відправників і шахрайських повідомлень;

- важливості оновлення антивірусного програмного забезпечення та правил перевірки робочої станції або інших пристроїв на встановлення актуального антивірусного захисту;
- про небезпеку завантаження файлів з невідомих або підозрілих джерел;
- про ознаки небезпечного шкідливого програмного забезпечення, яке може обійти антивірусний захист або загроз «нульового дня»;
- важливість регулярного резервного копіювання критично важливих даних і зберігання даних в безпечному місці;
- дотримання правил антивірусного захисту при дистанційній роботі;
- про шкоду, яку можуть заподіяти віруси, трояни, хробаки та інше шкідливе програмне забезпечення;
- правила дій у разі, якщо виявлено шкідливе програмне забезпечення на робочій станції.

### **Дотримання паролівної політики**

У рамках вищезазначеної навчальної програми з безпеки та нагадувань про безпеку працівників відповідальний за ІБ проводить навчання щодо дотримання паролівної політики. Таке навчання стосується правил призначення та зміни паролів, а саме:

- необхідність зміни паролів кожні щонайменше 90 днів;
- користувач не може повторно використовувати останні 3 паролі;
- паролі повинні містити не менше восьми символів і містити літери латинського алфавіту (верхнього регістру), малі та великі літери, цифри та спеціальні символи;
- заборону вживання прізвищ, імен, дат днів народження або номерів телефонів для призначених паролів;
- негайній зміні паролю при його компрометації або розголошенні;
- заборону передачі паролів іншим працівникам та стороннім особам, включаючи членів родини;
- заборону на запис паролів на папері, у робочому блокноті та іншому незахищеному місці біля робочої станції;
- заборону на завантаження, онлайн використання чи входу до стороннього програмного забезпечення та/або входу до інтернет-сайтів з автоматичним завантаженням паролів під час наступного доступу до цих ресурсів.

Будь-який працівник, якому відповідальний з ІБ доручив змінити свій пароль, тому що призначений пароль не відповідав вищезазначеним стандартам, повинен зробити це негайно.

## **11. РЕАГУВАННЯ НА ІНЦИДЕНТ**

### **Повідомлення про порушення**

1. Будь-який працівник, якому стало відомо про порушення політик інформаційної безпеки або про інцидент інформаційної безпеки, негайно повідомляє про це свого безпосереднього керівника та/або відповідального за ІБ.
2. Повідомлення повинно відбуватися негайно після виявлення можливого порушення або до закінчення робочого дня, якщо інші обов'язки заважають зробити це негайно.
3. Безпосередній керівник або відповідальний за ІБ перевіряє обставини можливого порушення та невідкладно вживає можливі заходи реагування на порушення, а також доповідає про порушення міському голові або його заступникам.
4. Для негайного повідомлення про порушення персонал може зателефонувати відповідальному за інформаційну безпеку.

### **Реагування на інцидент**

Відповідальний за інформаційну безпеку при отриманні повідомлення про порушення або інцидент самостійно або із залученням відповідних працівників вживає наступні заходи, з метою обмеження наслідків порушення чи інциденту:

1. Вживає заходів по збиранню та збереженню доказів та припиняє несанкціоновану дію.
2. Відключає або локалізує ІТ-систему, яка може бути уражена.
3. По можливості відновлює записи, дані, що могли постраждати.
4. По можливості усуває вразливості та слабкі місця, які призвели до інциденту.
5. Згідно плану реагування на кіберінциденти, повідомляє правоохоронним органам (CERT-UA, MISP UA тощо) про інцидент безпеки та його ознаки.

### **Розслідування та мінімізація ризиків**

1. При інциденті інформаційної безпеки, що може причинити значні негативні наслідки, відповідальний за ІБ долучає до розслідування відділ ІТ та керівника відділу/підрозділу де трапився інцидент.

2. Група розглядає обставини, причини та наслідки інциденту та оцінює ризики інформаційної безпеки, які пов'язані з інцидентом. При цьому розглядаються наступні фактори, але не обмежуються ними:

- характер цифрового активу, який постраждав внаслідок інциденту та його важливість для функціонування міської ради;
- необхідні заходи та засоби для відновлення функціонування;
- договірні зобов'язання, які можуть бути не виконані, порушені;
- ризики крадіжки особистих даних або втрати інформації внаслідок її псування, затирання чи шифрування, можливості щодо відновлення якомога актуальнішої версії резервного копіювання;
- ризик заподіяння фізичної шкоди, якщо втрата даних ставить під загрозу життя людини;
- ризик заподіяння шкоди репутації;
- обсяги (масив) втраченої, вкраденої чи зіпсованої інформації та кількість постраждалих осіб.

### **Профілактика**

1. Після вжиття негайних заходів для зменшення ризиків, пов'язаних з порушенням, відповідальний за ІБ проводить розслідування причин порушення.

2. При необхідності може проводитися аудит безпеки фізичних, організаційних і технологічних заходів. Це також може включати перегляд політики інформаційної безпеки.

3. Для проведення розслідування причин інциденту відповідальний за ІБ залучає відповідних працівників та при необхідності зовнішніх експертів.

4. Результати розслідування доповідаються міському голові або його заступникам разом з рекомендаціями, щодо запобігання подібних інцидентів у майбутньому.

5. За результатами складається план заходів з усунення недоліків, виявлених в ході розслідування інциденту, якщо це доречно.

### **Відповідальність**

Відповідальний за ІБ несе відповідальність за захист даних та підтримку належного рівня інформаційної безпеки. Керівництво та всі працівники, які порушують політику інформаційної безпеки та/або чинне законодавство несуть дисциплінарну, адміністративну чи кримінальну відповідальність.

**Керуюча справами  
виконавчого комітету**

**Антоніна НІКІТЧЕНКО**

**ЗАТВЕРДЖЕНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ**

Нижче наведений перелік затвердженого для використання програмного забезпечення, яке повинно бути встановлене на робочих станціях та використовуватись персоналом для роботи. Використання не затвердженого програмного забезпечення на робочих станціях заборонено.

<b>№ з/п</b>	<b>Тип програмного забезпечення</b>	<b>Назва програмного забезпечення</b>	<b>Версія</b>	<b>Безкоштовно (Так/Ні)</b>
1	Операційна система для персонального комп'ютера або ноутбука	Microsoft Windows	10 Pro 11 Pro	Ні
2	Програмне забезпечення для діловодства	Microsoft Office	2021 Pro	Ні
3	Антивірусне програмне забезпечення	ESET Nod	12	Ні
4	Програмне забезпечення для доступу в інтернет	Google Chrome	Остання	Так
5	Програмне забезпечення для багатофункціонального пристрою або принтера+сканера	Драйвер пристрою від виробника або з комплекту Microsoft Windows	-	Так (поставляється разом з пристроєм або з операційною системою)
6	Файловий архіватор	7-Zip	Остання	Так
7	Програмне забезпечення для відтворення відео-файлів	Media Player Classic	Остання	Так
8	Програмне забезпечення для проведення онлайн конференцій	Zoom	Остання	Так
9	Програмне забезпечення для проведення онлайн конференцій	Microsoft Teams	Остання	Так
10	Програмне забезпечення для проведення онлайн конференцій	Webex	Остання	Так
11	Комплекс програмних засобів потрібних для роботи програмного забезпечення	Java	Остання	Так
12	Комплекс програмних засобів потрібних для роботи програмного забезпечення	Microsoft .NET Framework	Остання	Так



**ФОРМА ЗАПИТУ НА ДОСТУП****(запит працівника чи підрядника на доступ до інформаційних ресурсів)**

ПІБ \_\_\_\_\_

Посада \_\_\_\_\_

Дата початку доступу \_\_\_\_\_

Режим доступу (цілодобовий чи у певні робочі години) \_\_\_\_\_

Дата та час припинення доступу \_\_\_\_\_

**Перелік ресурсів до яких надається доступ з вказанням прав доступу (читання, редагування, здачі під охорону сигналізацію, відвідування у вихідні дні тощо)**

1. Електронна пошта \_\_\_\_\_

2. Електронні реєстри \_\_\_\_\_

3. ІТ-системи, мережі \_\_\_\_\_

4. Програмне забезпечення, додатки \_\_\_\_\_

5. Віддалений доступ \_\_\_\_\_

6. Службовий телефон \_\_\_\_\_

7. Доступ до будівлі \_\_\_\_\_

**Погодження безпосереднього керівника** \_\_\_\_\_**Погодження відповідального за ІБ** \_\_\_\_\_