Номер	Назва	Опис
1	Назва органу ОМС	Баштанська міська рада
2	Дата останньої редакції	07.07.2025 р.
3	Власник документа	Баштанська міська рада
4	Дата затвердження	07.07.2025 р.
5	Дата набрання чинності	07.07.2025 р.

6	Відповідальний за інформаційну безпеку	Черін Андрій Анатолійович
7	Постачальник и послуг	Інтернет провайдер “Укертелеком”, «Цифрові технології», «Хоум-Нет»
8	Час блокування екрану	10 хвилин
9	Електронний зв'язок, електронна пошта, користування Інтернетом	bashtanskaotg@mk.gov.ua Інтернет провайдер “Укертелеком”, «Цифрові технології», «Хоум-Нет»
10	Аудит ідентифікаторів входу	Раз на рік
11	Блокування користувача	Після трьох невдалих спроб
12	Довжина пароля	Не менше 10 символів
13	Зміна пароля	90 діб

14	Повторне використання пароля	3
15	Антивірусне програмне забезпеченн я	**Cisco, Microsoft defender**
16	Виробник Антивірусного ПЗ	«Cisco», «Microsoft»,
17	Оновлення антивірусу	Автоматичне оновлення

18	Система фізичної безпеки	НІ
19	Час роботи	17:00 - 8:00
20	Безпечні двері	НІ
21	Детектори руху	ТАК
22	Датчики скла	НІ
23	Камери відеоспостереження	НІ
24	Надане обладнання	Комп’ютерна техніка з доступом до мережі інтернет
25	Віддалене блокування екрана	5 хвилин.
26	Збереження записів	5 років.
27	Контактний номер телефону	+380978895394

БАШТАНСЬКА МІСЬКА РАДА

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
Баштанської міської ради

ДАТА ОСТАННЬОЇ РЕДАКЦІЇ
04 ЛИПНЯ 2025 РОКУ

Дата **Підпис**

ЗМІСТ

Баштанська міська рада Політика інформаційної безпеки	
Назва: ВВЕДЕННЯ	**п 1.1 – 1.5**
Дата затвердження: «07» липня 2025 р.	**Огляд: Щорічний**
Дата набрання чинності: «07» липня 2025 р.	**Інформаційна безпека**

1. ВВЕДЕННЯ

1.1. Загальні положення

Ця політика інформаційної безпеки визначає основні засади забезпечення належного рівня інформаційної безпеки Баштанської міської ради, далі – Політика або скорочено ПІБ. ПІБ служить центральним програмним документом з інформаційної безпеки, з яким повинні бути ознайомлені всі працівники міської ради, підрядники (постачальники послуг), і визначає дії, застереження, заборони, яких повинні дотримуватися всі користувачі інформаційних та цифрових активів міської ради. Політика роздруковується та затверджується керівником Баштанської міської ради та зберігається у відповідального за інформаційну безпеку. У разі неможливості призначити окремого відповідального за інформаційну безпеку із-за обмеженості людського ресурсу, функцію відповідального за інформаційну безпеку виконує начальник відділу.

Належний рівень інформаційної безпеки, це такий стан фізичного, інформаційного середовища та середовища користувачів інформаційних та цифрових активів Баштанської 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 ПІБ, 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 управління. Цієї політики повинні дотримуватися всі штатні та тимчасові працівники в усіх місцях (на робочому місці, в будівлі ОМС чи працюючи віддалено), а також підрядники – постачальники послуг, які працюють з ОМС.

1.2. Глосарій

1.2.1. Загальні терміни та абревіатури, які використовуються в цьому документі.

Актив – матеріальні та нематеріальні об’єкти або інформація, що мають цінність для ОМС.

Брандмауер – спеціальне обладнання або програмне забезпечення, що працює на комп'ютері, яке дозволяє або відмовляє в проходженні трафіку через нього, на основі набору правил.

ВІБ – відповідальний за інформаційну безпеку, призначена особа, яка відповідає за впровадження та дотримання Політики інформаційної безпеки в ОМС. У разі неможливості призначити окремого відповідального за інформаційну безпеку, його функцію виконує начальник відділу.

Вірус – шкідливе програмне забезпечення, здатне відтворювати сама себе і зазвичай здатне завдати великої шкоди файлам або іншим програмам на комп'ютері, який воно атакує.

Доступність інформації – властивість, яка гарантує те, що забезпечується своєчасний доступ авторизованих осіб та процесів до інформації, а також відсутні простої в процесі її обробки, тобто коли інформація знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і у той час, коли вона йому необхідна. У випадку втрати інформації існує можливість своєчасного її відновлення.

ОМС – органи місцевого самоврядування.

Зовнішні носії інформації – компакт-диски, DVD-диски, дискети, флешки, USB, флеш-накопичувачі, касети та інші.

ІБ - Інформаційна безпека, це процес, який забезпечує збереження визначених Політикою безпеки властивостей інформації та спрямований на запобігання несанкціонованим діям в інформаційній системі, що включає сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи інформаційної системи.

ІС – Інформаційна система, організаційно-технічна система, у якій реалізується технологія обробки інформації з використанням технічних і програмних засобів.

ІТ – Інформаційна технологія.

Конфіденційність інформації – властивість, яка гарантує те, що доступ до інформації можуть одержати тільки авторизовані особи або процеси.

Користувач - Будь-яка особа зі складу працівників міської ради, уповноважена на доступ до певного інформаційного ресурсу.

Користувачі з можливостями запиту (лише для читання) – особи, яким на основі прав доступу заборонено додавати, видаляти або змінювати записи в базі даних та інших доступних їм масивах інформації. Їх системний доступ обмежується лише зчитуванням інформації.

Користувачі з можливостями редагування/оновлення – особи, яким дозволено на основі прав доступу додавати, видаляти або змінювати записи в базах даних та інших масивах інформації ОМС.

Локальна мережа – комп'ютерна мережа омс.

ПІБ – Політика інформаційної безпеки, це центральний, програмний документ, який визначає

основні засади забезпечення належного рівня інформаційної безпеки управління.

Персонал – всі працівники міської ради, які використовують інформаційні ресурси, комп'ютерне, телекомунікаційне і офісне обладнання відповідно до своїх посадових обов'язків.

ПК – персональний комп'ютер.

Привілейовані користувачі – системні адміністратори та інші особи, які конкретно ідентифіковані та мають санкціонований керівництвом доступ до певних баз даних та масивів інформації.

РГІБ – робоча група з інформаційної безпеки, колективний керівний орган системи управління інформаційною безпекою ОМС.

Спостережність системи - властивість, що дозволяє фіксувати діяльність користувачів і процесів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки або забезпечення відповідальності за певні дії.

СУІБ - Система управління інформаційною безпекою, це комплекс організаційних, програмних, технічних і фізичних заходів, спрямованих на управління ризиками, що пов'язані з використанням в управлінні інформації та інформаційних технологій.

Третя сторона – фізична чи юридична особа, яка перебуває у будь-яких договірних відносинах з ОМС та є стороною таких відносин.

Цілісність інформації – властивість, яка гарантує те, що інформація не містить помилок, є актуальною, вичерпною, будь-які зміни інформації здійснюються авторизованими особами чи процесами.

Шифрування – процес перетворення інформації, використовуючи алгоритм, щоб зробити її нечитабельною для будь-кого, крім тих, хто має авторизовану «потребу знати».

VLAN – Віртуальна локальна мережа – локальна мережа, яка використовується для сегментації мережевого трафіку з метою адміністрування та безпеки.

VPN – Віртуальна приватна мережа – забезпечує безпечну передачу даних та доступ через загальнодоступні мережі.

Інші терміни, що вживаються у цій Політиці, застосовуються в значеннях, визначених чинним законодавством України.

1.3. Застосовані положення

Нижче наведено перелік нормативних та регулюючих законів, актів, стандартів на основі яких розроблено цей документ.

1. Закон України «Про основні засади забезпечення кібербезпеки України»;
2. Закон України «Про інформацію»;
3. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»;
4. Закон України «Про електронні документи та електронний документообіг»;
5. Постанова КМУ №518 від 19.06.2019 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури»;
6. ISO/IEC27000:2019 - Інформаційні технології - Методи і засоби забезпечення безпеки - Системи управління інформаційною безпекою - Загальні відомості і словник;
7. ISO/IEC 27001:2013 - Інформаційні технології - Методи захисту - Системи управління інформаційною безпекою – Вимоги;
8. ISO/IEC 27002:2013/COR 2:2015 - Інформаційні технології - Методи захисту - Звід рекомендованих правил для управління інформаційною безпекою;
9. ISO/IEC 27003:2017 - Інформаційні технології - Методи безпеки - Системи управління інформаційною безпекою – Керівництво;
10. ISO/IEC 27004:2016 - Інформаційні технології - Методи безпеки - Управління інформаційною безпекою - Моніторинг, вимір, аналіз і оцінка;
11. ISO/IEC 27005:2018 - Інформаційні технології - Методи безпеки - Управління ризиками інформаційної безпеки;
12. ISO/IEC 15408-1:2009 - Загальні критерії оцінки захищеності інформаційних технологій;
13. ISO/IEC TS 27008:2019 - Методи безпеки - Вказівки для оцінки засобів контролю інформаційної безпеки;
14. ISO 27032 – Інформаційні технології. Методи захисту;
15. ISO 27035 – Управління інцидентами

Баштанська міська рада	Політика інформаційної безпеки
Назва: ОБОВ'ЯЗКИ ПРАЦІВНИКІВ	**п 2.1 -2.9**
Дата затвердження: 07.07.2025 р	**Огляд: Щорічний**
Дата набрання чинності: 07.07.2025 р.	**Інформаційна безпека, людські ресурси**

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 міської ради є вжиття необхідних заходів для забезпечення фізичної безпеки активів міської ради. 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 ВІБ або охорону міської ради при наявності служби охорони.

Захист робочих станцій. Всі робочі станції (ПК), які знаходяться в закладі не повинні залишати міську раду без відповідного дозволу керівника чи ВІБ. Всім новим користувачам надається перший інструктаж на робочому місці щодо правил використання та зберігання робочих станцій управління. Більшість ПК міської ради містять конфіденційні дані кадрового чи фінансового характеру, тому слід дотримуватися максимальної обережності, щоб ці дані не були скомпрометовані. При використані робочих станцій за межами Баштанської міської ради користувач повинен вжити всіх можливих заходів із забезпечення безпечного зберігання та використання ПК, інформації та програмного забезпечення, 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 ВІБ.

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 міської ради тільки таке комп'ютерне обладнання та програмне забезпечення, яке дозволено використовувати. На ПК, що

дистанційно підключається до локальної мережі міської 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 Баштанської міської ради, є власністю міської ради, якщо інше не передбачено умовами відповідного договору. Право власності управління на програмні засоби зберігається у разі їх офіційного обліку та затвердження відповідним актом (наприклад, актом модернізації 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 СУІБ.
- 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 ПІБ процедурою, суворо заборонено.
- Використання особистого або недозволенного програмного забезпечення на робочих станціях. Використання особистого або недозволенного програмного забезпечення на робочих станціях міської ради заборонено. Все програмне забезпечення, встановлене на робочих станціях, має бути затверджене та дозволене до використання.
- 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 не належним 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 Баштанській міській раді, або обробляються на пристроях, що належать міській раді, вважаються власністю Баштанської 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 управління,
- не порушує нічого з наступного:

1) Незаконна діяльність - використання інформаційних ресурсів Баштанської 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 Баштанської міської ради для отримання особистої вигоди суворо заборонено.
3) Політична діяльність – Вся політична діяльність суворо заборонена в приміщеннях та з використанням інформаційних ресурсів Баштанської міської ради. Заклад заохочує своїх працівників голосувати та активно брати участь у виборчому процесі, але ці заходи не повинні виконуватися з використанням активів та ресурсів Баштанської 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 Баштанської 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.

Заклад зберігає за собою право здійснювати моніторинг змісту будь-якого електронного повідомлення та комунікації, що генерується або передається з використанням інформаційних активів Баштанської 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, для аудиту або аналізу витрат на зв'язок, можуть відстежуватися набрані номери зі службових телефонів, тривалість дзвінків, кількість дзвінків на/з конкретного телефону, час доби і т.д. Інші приклади, 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.

Заклад 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.

2.4 Доступ до мережі Інтернет

Доступ в Інтернет надається тільки тим співробітникам, хто його потребує для виконання службових обов'язків. Доступ до Інтернет це ресурс, за який Баштанська міська рада витрачає кошти тому його використання потребує виконання наступних вимог. 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 збільшує витрати міської ради, а також 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 і може бути звільнений.

В закладі 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 міської 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 про Баштанську міську раду була доступна в Інтернеті;
- контролює, щоб користувачі не мали прав встановлювати або завантажувати будь-яке програмне забезпечення (додатки, медіа файли, заставки тощо) з Інтернет. Якщо у користувачів є потреба в додатковому програмному забезпеченні, користувач повинен отримати дозвіл;
- використання Інтернету повинно узгоджуватися з комерційною діяльністю ОМС. Мережа може бути використана для продажи послуг, однак 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 ІБ. Самостійне використання шифрувального програмного забезпечення та ключів шифрування, без погодження з відповідальним за ІБ, заборонено, і може призвести до дисциплінарного покарання.

2.5. Повідомлення про несправності

Користувачі повинні інформувати ІТ 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 ІТ-підрозділ та відповідального за ІБ, 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 з ІБ повинен вжити заходи для усуненням несправності, а також повідомити

керівнику 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 міської ради або підрядники, які мають доступ до цифрових активів Баштанської міської ради зобов'язані повідомляти відповідального з ІБ про виявлені інциденти інформаційної безпеки. Користувач - це будь-яка особа, уповноважена на доступ до інформаційного ресурсу ОМС. 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. При неможливості негайного повідомлення про інцидент безпеки вищевказаним особам, користувач повинен без зволікань проінформувати про інцидент будь-якого члена Робочої групи з інформаційної безпеки ОМС, які вказані вище в цьому документі.

Реагування на повідомлення про інциденти інформаційної безпеки повинно бути якомога швидким. Кожен член Робочої групи з інформаційної безпеки повинен 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 Баштанської міської ради. Усі виявлені інциденти реєструються в журналі інцидентів інформаційної безпеки. 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 Баштанської 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 IT-системи, фінансову інформацію або дані про людські ресурси, не повинні розміщуватися на будь-якому комп'ютері, який не є власністю управління, без письмової згоди відповідного керівника відділу, який повинен захищати всі дані та програмне забезпечення, які йому належать, тому повинен контролювати системи, в яких такі дані містяться. У випадку, якщо відповідний керівник отримає 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 заклад обмежений у можливостях захисту даних на персональних ПК тому дозвіл на переміщення треба надавати у разі гострої службової необхідності. Заклад не може бути впевнений 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 конфіденціальності та захисту конфіденційної інформації при передачі в мережі Інтернет дозволяється використання відповідного програмного забезпечення (наприклад програми WinZip), 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 WinZip) 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 WinZip).

Баштанська міська рада	Політика інформаційної безпеки
Назва: УПРАВЛІННЯ ДОСТУПОМ	**П 3.1 – 3.6**
Дата затвердження: 07.07.2025 р	**Огляд: Щорічний**
Дата набрання чинності: 07.07.2025 р	**Інформаційна безпека управління 1 категорії**

3. УПРАВЛІННЯ ДОСТУПОМ

3.1. Ідентифікація користувачів

Кожний користувач повинен мати унікальний ідентифікатор (обліковий запис, логін) та пароль для входу. Система контролю доступу повинна ідентифікувати кожного користувача і запобігати доступу та використанню інформаційних ресурсів Баштанської міської ради неавторизованим користувачем. Вимоги безпеки для ідентифікації користувача включають:

- кожному користувачеві присвоюється унікальний ідентифікатор;
- користувачі несуть відповідальність за використання та неправомірне використання свого індивідуального ідентифікатору.

Усі ідентифікатори входу користувачів перевіряються щонайменше раз на рік і всі неактивні ідентифікатори блокуються. Відділ кадрів міської ради сповіщає відповідального за ІБ або відповідного фахівця ІТ-відділу про звільнення працівника або припинення співробітництва з персоналом підрядника. При отримані такого сповіщення неактивні ідентифікатори блокуються.

Ідентифікатор входу блокується після максимум трьох (3) невдалих спроб входу в систему. Для відновлення доступу в цьому випадку потрібне призначення нового тимчасового паролю Адміністратором.

Користувачі, які бажають отримати доступ до систем та мереж управління, повинні заповнити відповідну Форму Доступу (Додаток 1). Ця форма повинна бути підписана безпосереднім керівником та санкціонована керівником міської ради або відповідальним за інформаційну безпеку.

3.2. 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 призначені паролю користувачеві буде автоматично запропоновано вручну призначити пароль, відповідно до таких вимог:

Довжина пароля – Пароль повинен складатися з мінімуму десять (10) 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 60 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.

3.3. Угода про конфіденційність

Користувачі інформаційних ресурсів Закладу при працевлаштуванні підписують угоду про конфіденційність (Додаток 2). 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 ОМС.

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

3.4. Контроль доступу

Інформаційні ресурси управління захищаються за рахунок використання системи контролю доступу. Система контролю доступу включає внутрішні засоби захисту (паролі, шифрування, таблиці контролю доступу, налаштування інтерфейсів користувача тощо), так і зовнішні (пристрої захисту портів, брандмауери, автентифікацію на основі хоста тощо).

Правила доступу до ресурсів встановлюються власником ресурсу. Доступ надається тільки шляхом заповнення форми запиту на доступ (Додаток 1). Ця форма затверджується керівником міської ради чи відповідальним з ІБ.

При наданні доступу використовується принцип мінімально необхідного доступу до ресурсу користувача для виконання ним функціональних завдань. Доступ користувача до відповідного ресурсу відбувається тільки після затвердження форми запиту на доступ міським головою чи відповідальним з інформаційної безпеки та тільки до того ресурсу до якого був наданий запит на допуск.

В закладі можуть використовуватись випливаючи на екрані робочих станцій електронні попередження про несанкціоноване використання ресурсу та про відповідальність порушника.

При використанні програмного забезпечення управління безпекою кінцевих пристроїв повинна підтримуватися онлайн авторизації при використані додатків. Кожне підключення підлягає процесу авторизації (введенню логіна та пароля).

3.5. Припинення права доступу

Якщо працівник змінює посаду його безпосередній керівник ініціює перегляд прав доступу та заповнює Форму запиту на доступ (Додаток 1). У Формі вказується дата набрання чинності зміни посади та назва посади, щоб ІТ-відділ міг змінити права доступ відповідно до принципу мінімально необхідного доступу до ресурсів. Протягом обмеженого періоду працівнику, який змінює посаду, можуть зберігатися попередні права доступу, а також додаватися нові права доступу, необхідні для виконання нових посадових обов'язків.

Перегляд прав доступу працівникам повинен проводитися не рідше ніж раз на рік. Відповідальний за інформаційну безпеку повинен сприяти перегляду прав доступу користувачів, щоб переконатися, що весь персонал має мінімально необхідні права доступу для ефективного виконання своїх робочих функцій. Виявлені в ході перегляду надлишкові права доступу повинні припинятися.

3.6. Припинення дії облікового запису користувача

При звільненні працівника, його безпосередній керівник повинен завчасно ініціювати процедуру припинення доступу, вказавши «Видалити доступ» у Формі запиту на доступ (Додаток 1) та дату останнього робочого дня працівника, щоб його обліковий запис користувача міг бути налаштований на закінчення терміну дії у день звільнення. Безпосередній керівник контролює своєчасну здачу працівником, що звільняється відповідних пристрої доступу, які йому/їй надавалися. Обліковий запис та доступ працівника блокується по завершенні останнього робочого дня.

Не рідше одного разу на рік, відповідальний з інформаційної безпеки повинен ініціювати перегляд списку активних облікових записів користувачів для оцінки прав доступу відповідно до принципу надання мінімально необхідного доступу до ІТ-ресурсів для виконання функціональних завдань. Керівники відділів міської ради повинні переглянути списки доступу стосовно своїх підлеглих та протягом п'яти (5) робочих днів надати уточнюючі дані щодо прав доступу. Якщо буде виявлені надлишкові права доступу вони повинні бути припинені. Про необхідність припинення надлишкових прав доступу або блокуванні активних акаунтів звільнених працівників керівники відділів без зволікань повідомляють ІТ-відділ та надають оновлену Форму запиту на доступ (Додаток 1).

Баштанська міська рада	Політика інформаційної безпеки
Назва: ПІДКЛЮЧЕННЯ ДО МЕРЕЖІ	**П 4.1 – 4.5**
Дата затвердження: 07.07.2025 р.	**Огляд: Щорічний**
Дата набрання чинності: 07.07.2025 р.	**Інформаційна безпека управління 1 категорії**

4. ПІДКЛЮЧЕННЯ ДО МЕРЕЖІ

4.1. З’єднання та підключення

Доступ до інформаційних ресурсів управління через модеми, інші комунікаційні пристрої або відповідне програмне забезпечення підлягає авторизації та автентифікації системою контролю доступу. Зовнішній виклик чи комутація на внутрішній номер (кінцевий пристрій) 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 начальника відділу з поданням Форми доступу (Додаток 1) та затверджуються міським головою чи 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 міського голови або відповідального з ІБ. При прийняті 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:

- телефонні лінії та обладнання
- факсимільні лінії та обладнання
- телефоні навушники та гарнітура
- телефони типу програмного забезпечення, встановлені на робочих станціях
- службові мобільні телефони
- програмне забезпечення для маршрутизації викликів
- обладнання для адміністрування телефонної системи

- мережеві лінії
- міжміські лінії
- місцеві телефонні лінії.

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 підключені 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 міської ради. Відповідальний за інформаційну безпеку повинен бути залучений до процесів проектування та затвердження каналів підключення до зовнішніх мереж, а також укладення договорів з третьою стороною на отримання послуг з телекомунікаційного забезпечення міської ради.

4.4. Договір на телекомунікаційні послуги

При укладанні договору на отримання телекомунікаційних послуг закладом 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 міської ради;
- 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 управління 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.

Баштанська міська рада	Політика інформаційної безпеки
Назва: Антивірусний захист	П 5.1 – 5.3
Дата затвердження: 07.07.2025 р	**Огляд: Щорічний**
Дата набрання чинності: 07.07.2025 р.	**Інформаційна безпека управління 1 категорії**

5. АНТИВІРУСНИЙ ЗАХИСТ

5.1. Встановлення та оновлення антивірусного ПЗ

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

Конфігурації **-** антивірусне програмне забезпечення, яке на даний час використовується, є Cisco. Оновлення надходять безпосередньо від Cisco. 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 закладі ведеться контроль оновлення та застосування антивірусного програмного забезпечення. ІТ-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 міської ради використовується лише дозволене до використання програмне забезпечення. Встановлення нового програмного забезпечення потребує отримання дозволу голови міської ради або відповідального з інформаційної безпеки. Перелік дозволеного до використання програмного забезпечення наведений у Додатку 3. Перед встановленням нове програмне забезпечення проходить перевірку ІТ-підрозділом з метою забезпечення сумісності зі встановленим на даний момент програмним забезпеченням і конфігурацією мережі. Крім того, ІТ- підрозділ повинен перевірити нове програмне 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 (загально доступного джерела) та може мати віруси та інше шкідливе програмне забезпечення, перед його встановленням на комп'ютерах міської ради 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 міської ради з іншого місця, повинні бути перевірені на віруси відразу після отримання. Перевірку та сканування на віруси здійснює ІТ-підрозділ за допомогою наявного антивірусного програмного забезпечення.

Кожна дискета, компакт-диск, DVD і USB-пристрій є потенційним джерелом комп'ютерного вірусу. Тому такі зовнішні носії інформації повинні бути про скановані на наявність вірусів та іншого шкідливого програмного забезпечення, перш ніж інформація з них буде скопійована на комп'ютери ОМС.

Забороняється завантажувати комп'ютери з дискети, компакт-диска, DVD або USB-пристрою, отриманого із зовнішнього джерела. Користувачі завжди повинні видаляти будь-яку зовнішні носії з комп'ютера, коли він не використовується. Це робиться для того, щоб дискета, компакт- диск, DVD або 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 міської ради, якщо на них не поширюється дія іншого договору. Програмні засоби, застосунки або документація які розробляються за замовленням міської ради є також його власністю. Розробники таких програмних продуктів та документації повинні підписати заяву, в якій визнається право власності управління на відповідний програмний продукт та документацію. Програмне забезпечення, придбане працівником за власний рахунок, залишається власністю працівника, який придбав це програмне забезпечення.

Баштанська міська рада	Політика інформаційної безпеки
Назва: КРИПТОГРАФІЧНИЙ ЗАХИСТ	**П 6.1 – 6.6.**
Дата затвердження: 07.07.2025 р.	**Огляд: Щорічний**
Дата набрання чинності: 07.07.2025 р.	**Інформаційна безпека управління 1 категорії**

6. КРИПТОГРАФІЧНИЙ ЗАХИСТ

6.1. Визначення

Криптографічний захист інформації за допомогою шифрування даних є найефективнішим способом забезпечення безпеки даних Баштанської 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 закладі використовуються наступні засоби криптографічного захисту: інфраструктура відкритих ключів з електронним цифровим підписом; програма – архіватор WinZip; програма «Криптоавтограф»; передача файлів за допомогою протоколу FTP; захищений веб-інтерфейс SSL.

6.2. Ключи 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 міською радою 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. Заклад 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 ідентифікованному зовнішньому користувачеві, може скористатися інфраструктурою відкритих ключів та електронним цифровим підписом (ЕЦП). Порядок використання ЕЦП у закладі повинно бути погоджено з керівником чи відповідальним за інформаційну безпеку.

6.4. Використання WinZip

Це програмне забезпечення дозволяє працівникам ОМС 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, мессенджер або телефоном. Працівник, який має потребу у передачі конфіденційної інформації віддаленому користувачу через Інтернет може запросити дозвіл на використання програми WinZip у відповідального з інформаційної безпеки. При цьому відповідальний з ІБ повинен також отримати пароль до зашифрованого архіву для перевірки інформації, що підлягає передачі чи отримується.

6.5. Протокол передачі файлів FTP

Користувач може передати файли зі своєї робочої станції на захищені sFTP-сайти за допомогою відповідних заходів безпеки. FTP (англ. File Transfer Protocol) або sFTP (Secure File Transfer Protocol) це стандартний мережевий протокол прикладного рівня призначений для пересилання файлів між клієнтом та сервером в комп'ютерній мережі. Клієнт та сервер створюють окремі канали для передачі даних та обміну командами. Можлива автентифікація клієнтів із використанням логіну та паролю користувача. Порядок FTP-передачі файлів повинен бути погоджений з керівником та відповідальним за інформаційну безпеку..

6.6. 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 інформації через веб-сторінку в Інтернеті при наданні/отриманні послуг онлайн. Порядок використання веб- інтерфейсу захисту SSL погоджується з керівником міської ради та відповідальним з інформаційної безпеки.

6.7. Використання програми «Криптоавтограф»

Комплекс програмний криптографічного захисту інформації "Крипто Автограф 2.0" (далі - Комплекс) призначений для експлуатації у якості засобу кваліфікованого електронного підпису (КЕП) чи печатки у взаємодії з пристроями створення безпечного підпису (захищеними носіями особистих ключів, токен, смарт-карта), а також для електронної ідентифікації, обчислення, перевірки та підтвердження кваліфікованого електронного підпису та кваліфікованої електронної печатки, шифрування даних, а також надання користувачам можливості отримання та використання електронних довірчих послуг.

Баштанська міська рада	Політика інформаційної безпеки
Назва: ФІЗИЧНА БЕЗПЕКА	**Розділ 7**
Дата затвердження: 07.07.2025 р	**Огляд: Щорічний**
Дата набрання чинності: 07.07.2025 р.	**Фізична безпека управління 1 категорії**

7. ФІЗИЧНА БЕЗПЕКА

Забезпечення фізичної безпеки працівниками полягає у створенні безпечних умов на робочому місці та одночасним забезпеченням безпечного зберігання активів міської ради. Будівля (комплекс будівель) міської ради є дещо унікальним місцем з точки зору прав власності на будівлю або умов договору оренди, території навколо, шляхів під'їзду/виїзду, зовнішнього огородження, входів у приміщення, вимог до пожежної безпеки, систем електроживлення, 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.

Міська рада обладнана системою резервного живлення, а саме дизель-генератором.

8. ДИСТАНЦІЙНА РОБОТА

В закладі 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) 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 міської ради.

8.1. Загальні вимоги

Користувачі, що працюють віддалено, зобов'язані дотримуватися всіх правил міської ради, 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 заклад не надасть все обладнання, необхідне для забезпечення належного захисту інформації, до якої працівник має доступ; однак є певний перелік обладнання який заклад повинен надати:

Заклад надає:

- робочий комп’ютер (ноутбук) зі встановленим антивірусним ПЗ та програмним забезпеченням шифрування даних;
- принтер;
- зовнішній носій для резервного копіювання;
- службовий мобільний телефон.

Працівник повинен забезпечити самостійно:

- широкосмуговий канал доступу до Інтернет;
- подрібнювач паперу або можливість іншим способом знищувати паперові носії;
- відокремлене від членів родини робоче місце;
- 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 міської ради і налаштоване на періодичне оновлення. Заборонено працювати без оновленого антивірусного програмного забезпечення.

Використання VPN та брандмауера**:** При дистанційному підключені повинен використовуватись канал зв'язку, який вимагає використання VPN та брандмауера. При відключені 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 закладом 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, треба звернутися до IT- сектору міської ради. При гострій необхідності та неможливості звернутися до IT-підрозділу (наприклад під час відрядження) дозволено використовувати наявні засоби шифрування (архіватор-шифрувальник WinZip) та доступний зовнішній носій. Причому, безпечному зберіганню зовнішнього носія з резервною копією даних треба приділити значну увагу.

Передача даних**:** Передача даних до управління 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 до міської ради.

Доступ до зовнішніх систем (хмар): Якщо є потреба у доступі до зовнішньої IT-системи, необхідно

зв'язатися зі своїм безпосереднім керівником або відповідальним за інформаційну безпеку. Вони визначать безпечний метод доступу до потрібної зовнішньої системи.

Електронна пошта: Не дозволено передавати будь-яку конфіденційну інформацію та персональні дані (перелік визначений у п.2.9 цього документу) електронною поштою, якщо вона не зашифрована. При гострій необхідності треба звернутися до свого безпосереднього керівника або відповідального за інформаційну безпеку. Вони визначать безпечний метод передачі конфіденційної інформації та персональних даних електронною поштою.

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

Захистить 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 управління**:** Вся передача даних за межі міської ради 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. Інший спосіб утилізації - такі документи палити. Персонал, який працює дистанційно повинен мати або подрібнювач паперу або можливість палити паперові документи.

Зовнішні носії: Всі зовнішні носії надані закладом для забезпечення дистанційної роботи повинні бути повернуті до міської ради для утилізації.

Баштанська міська рада	Політика інформаційної безпеки
Назва: ПОЛІТИКА ЧИСТОГО СТОЛУ/ЕКРАНУ	**Р. 9**
Дата затвердження: 07.07.2025 р.	**Огляд: Щорічний**
Дата набрання чинності: 07.07.2025 р.	**Інформаційна безпека управління 1 категорії**

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 Баштанську міську раду від витоку конфіденційної інформації.

Метою впровадження політики чистого столу та чистого екрану в Баштанської міської ради є:

- запобігання витоку/втраті конфіденційних даних ОМС;
- 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 Баштанської міської ради. Усі працівники Баштанської міської ради мають бути ознайомлені із її вимогами. До будь-якого працівника ОМС, визнаного винним у порушенні цієї політики, може бути застосована дисциплінарна практика, аж до звільнення.

Вимоги

Увесь персонал ОМС 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 вимкнуто 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.

Добавлено примечание ([1]): можливо краще мобільний телефон?

Добавлено примечание ([2]): @dmitro.gavriliak@gmail.com чисто технічно це може бути 7-ми дюймовий планшет , який легко поміщається в карман звичайної куртки , тому я б залишив отак як є

Баштанська міська рада	Політика інформаційної безпеки
Назва: Обізнаність та навчання з питань безпеки	**Р 16**
Дата затвердження: 07.07.2025 р	**Огляд: Щорічний**
Дата набрання чинності: 07.07.2025 р	**Інформаційна безпека управління 1 категорії**

10. ОБІЗНАНІСТЬ ТА НАВЧАННЯ З ПИТАНЬ БЕЗПЕКИ

Для підвищення обізнаності стосовно питань інформаційної безпеки весь персонал міської ради, 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 за інформаційну безпеку веде відповідну документацію про всі навчальні заходи.

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 поводження 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, якщо виявлено шкідливе програмне забезпечення на робочій станції

Дотримання парольної політики

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

- Необхідність зміни паролів кожні щонайменше 90 днів.
- Користувач не може повторно використовувати останні 6 паролів.
- 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 розголошені.
- Заборону передачі паролів іншим працівникам та стороннім особам, включаючи членів родини
- Заборону на запис паролів на папері, у робочому блокноті та іншому незахищеному місті 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.

Добавлено примечание ([3]): треба поставити 60 або 90 зміна кожні 30 призведе до деградації паролів

Баштанська міська рада	Політика інформаційної безпеки
Назва: ПЕРЕВІРКА КАНДИДАТІВ	**Р 19**
Дата затвердження: 07.07.2025 р	**Огляд: Щорічний**
Дата набрання чинності: 07.07.2025 р	**Інформаційна безпека управління 1 категорії**

11. ПЕРЕВІРКА КАНДИДАТІВ

Заклад проводить довідкові перевірки кандидатів перед працевлаштуванням. Від кандидата завчасно отримується згода на проведення такої перевірки. Кандидат, який відмовляється від такої перевірки, перестає бути кандидатом та його вивчення кадровим відділом припиняється.

Відділ кадрів збирає інформацію про репутацію кандидата, особисті характеристики або спосіб життя. Дана інформація може бути зібрана в Інтернеті, включаючи сайти соціальних мереж, через публічні чи освітні записи або через співбесіди з попередніми роботодавцями, партнерами, особами, що можуть надати рекомендаційні листи або будь ким іншим.

Ця інформація також може бути додатково переглянута під час здійснення працівником порушення або його/її перепризначення на посаду з розширенням прав доступу. Повідомлення про судимість не обов'язково дискваліфікує кандидата на працевлаштування. При прийнятті рішення враховується характер і серйозність правопорушення, дата правопорушення, обставини та можливі ризики для ОМС при працевлаштуванні такого кандидата.

Заклад має право відкликати пропозицію про працевлаштування, або звільнити працівника при виявлені свідомого надання неправдивої інформації стосовно себе.

Звіти про перевірку біографічних даних зберігається, як конфіденційна інформація відділом кадрів.

Баштанська міська рада	Політика інформаційної безпеки
Назва: Реагування на інцидент	**Р 20**
Дата затвердження: 07.07.2025 р	**Огляд: Щорічний**
Дата набрання чинності: 07.07.2025 р	**Інформаційна безпека управління 1 категорії**

12. РЕАГУВАННЯ НА ІНЦИДЕНТ

Повідомлення про порушення

1. Будь-який працівник, якому стало відомо про порушення політик інформаційної безпеки або про інцидент ІБ негайно повідомляє про це свого безпосереднього керівника та/або відповідального за ІБ.
2. Повідомлення повинно відбуватися негайно після виявлення можливого порушення або до закінчення зміни, 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 керівнику управління.
4. Для негайного повідомлення про порушення персонал може зателефонувати відповідальному за інформаційну безпеку за номером телефону 0978895394.

Реагування на інцидент

Відповідальний за інформаційну безпеку при отримані повідомлення про порушення або інцидент самостійно або із залученням відповідних працівників міської ради 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 кіберінцеденти, повідомляє правоохоронним органам (CERT-UA, MISP UA) про інцидент безпеки та його ознаки.

Добавлено примечание ([4]): тут повинна бути наша політика реагування на кіберінциденти

Розслідування та мінімізація ризиків

При інциденті інформаційної безпеки, що може причинити значні негативні наслідки відповідальний за ІБ долучає до розслідування членів Робочої групи з інформаційної безпеки. До РГІБ також долучається керівник відділу/підрозділу де трапився інцидент.

1. 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 ОМС;
    - 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 міської ради та при необхідності зовнішніх експертів.
4. Результати розслідування доповідаються керівнику міської ради 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

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

ДОДАТОК 1

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 _____

ДОДАТОК 2

Згода про нерозголошення

ВІДПОВІДАЛЬНІСТЬ ЗА РОЗГОЛОШЕННЯ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

Я розумію і погоджуюся зберігати, захищати та не розголошувати конфіденційну інформацію Баштанської міської ради. Крім того, я розумію, що будь-яке несанкціоноване використання або розголошення інформації міської ради , може призвести до дисциплінарної, адміністративної чи кримінальної відповідальності відповідно до політики інформаційної безпеки Баштанської міської ради та чинного законодавства.

_____ _____

Дата Підпис

_____ _____

Дата Підпис відповідального за ІБ

ДОДАТОК 3

ЗАТВЕРДЖЕНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

Нижче наведений перелік затверджено 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.

ПЗ	Версія	Затверджено	Дата	Опис/Коментарі

ДОДАТОК 4

ЗАТВЕРДЖЕНІ ПОСТАЧАЛЬНИКИ

Постачальник	Основний контакт	Основний номер	Товар/Послуга	Опис/Коментарі

ДОДАТОК 5

ЖУРНАЛ РЕЄСТРАЦІЇ ПОДІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

№	Назва події	Дата. Час	Ознаки/ індикатори	Вжиті заходи/ реагування	Рекомендації/ коментарі

ДОДАТОК 6

ЖУРНАЛ УПРАВЛІННЯ ЗМІНАМИ

Дата	Назва ПЗ/АЗ	Опис зміни	Створена РЗ до зміни	Зміна запроваджена з (дата, час)	Отримані відгуки/ скарги	Вжиті заходи	Коментарі

Прим. ПЗ – програмне забезпечення;

АЗ – апаратне забезпечення;

РК - резервна копія.

Додаток 7

Перелік програмного забезпечення та загальні вимоги до ліцензування програмного забезпечення типового робочого місця працівника Баштанської міської ради

Зміст

Перелік програмного забезпечення для типового робочого місця

В таблиці 1 наведено перелік програмного забезпечення для типового робочого місця в управлінні.

Таблиця 1. Перелік програмного забезпечення для типового робочого місця в ОМС

з/п	Тип програмного забезпечення	Назва програмного забезпечення	Безкоштовно (Так/Ні)
1	Операційна система для персонального комп'ютера або ноутбука	Microsoft Windows	Ні
2	Антивірусне програмне забезпечення	Windows Defender	Поставляється разом з операційною системою
3	Програмне забезпечення для доступу в інтернет	Google Chrome	Так Посилання
4	Програмне забезпечення для багатофункціонального пристрою або принтера + сканера	Драйвер пристрою від виробника або з комплекту Microsoft Windows	Поставляється разом з пристроєм або з операційною системою
5	Програмне забезпечення для діловодства	Microsoft Office	Ні
6	Антивірус	Cisco	Так

Загальні вимоги до програмного забезпечення, яке закуповується для ОМС

Тендерною документацією та договором про закупівлю програмного забезпечення повинне бути передбачено:

- забезпечення продавцем комплектності поставки програмного продукту, зазначений у специфікації, яка додається до договору;
- встановлення у разі потреби програмного забезпечення продавцем на технічних засобах покупця;
- надання продавцем гарантійних зобов'язань;
- визначення строків та умов технічної підтримки програмного забезпечення.

Специфікація на поставку програмного забезпечення, яка додається до договору, повинна передбачати наявність:

- електронного носія інформації з примірником програмного забезпечення, до якого у разі потреби додаються засоби для його встановлення на технічних засобах покупця;
- програмної та експлуатаційної документації на програмне забезпечення;
- ліцензії або іншого документа, що підтверджує правомірність використання програмного забезпечення.

Умови використання програмного забезпечення повинні передбачати, що строком ліцензії на використання програмного продукту є строк чинності виключних майнових прав інтелектуальної власності на відповідне програмне забезпечення.

У договорі про надання технічної підтримки програмного забезпечення повинне бути передбачено:

- перелік послуг з технічної підтримки програмного забезпечення з обґрунтуванням кошторисної вартості надання кожної з таких послуг;
- строки та порядок надання послуг;
- перелік випадків (обставин), настання яких є підставою для надання послуг на вимогу міської ради;перелік послуг (у разі наявності), які надаються безоплатно.

Загальні вимоги до ліцензування програмного забезпечення

Права інтелектуальної власності охоплюють авторське право на програмне забезпечення чи документ на авторське право, права на промисловий зразок, торгові марки, патенти і ліцензії на початковий текст.

Патентований програмний продукт постачають згідно з ліцензійною угодою, яка визначає терміни та умови ліцензії, наприклад, обмеження використання продуктів визначеними комп'ютерами або обмеження копіювання створенням лише резервних копій. Законодавчі, регуляторні та контрактні вимоги можуть накладати обмеження на копіювання конкретних патентованих матеріалів. Зокрема, вони можуть вимагати, що можна використовувати лише матеріал, розроблений закладом або який
ліцензовано чи надано управлінню розробником.

Порушення авторського права може призвести до втрати підтримки програмного продукту та судового позову, який може також включати штрафи або навіть кримінальне переслідування винних осіб.

Має бути впроваджено належні процедури забезпечення відповідності законодавчим, нормативним і контрактним вимогам щодо прав інтелектуальної власності та щодо використання запатентованих продуктів програмного забезпечення.

Для захисту будь-яких матеріалів, які можна вважати інтелектуальною власністю, треба розглядати наведені нижче настанови:

- публікація політики відповідності правам інтелектуальної власності, яка визначає правове використання програмного забезпечення та інформаційних продуктів;
- придбання програмного забезпечення лише через відомі та визнані джерела для забезпечення того, що авторські права не порушуються;

- підтримка поінформованості щодо політики захисту прав інтелектуальної власності та надання попередження про намір вжиття дисциплінарних дій проти працівників, які їх порушують;
- підтримка відповідних реєстрів ресурсів СУІБ та ідентифікація всіх ресурсів СУІБ з вимогами захисту прав інтелектуальної власності;
- підтримка доказів у вигляді договорів на закупівлю програмного забезпечення та свідоцтв володіння ліцензіями, майстер-дисків, настанов тощо;
- запровадження заходів безпеки для забезпечення того, щоб не було перевищено будь-якої кількості дозволених користувачів;
- виконання перевірок, що інстальовано лише санкціоноване програмне забезпечення та ліцензовані продукти;
- надання політики вилучення чи передавання програмного забезпечення іншим сторонам;
- відповідність термінам та умовам щодо програмного забезпечення та інформації, отриманих із загальнодоступних мереж;
- відсутність відмінного від дозволеного авторським правом дублювання, перетворення в інший формат або виділення з комерційних записів (кіно, аудіо);
- недопущення відмінного від дозволеного авторським правом повного або часткового копіювання книг, статей, звітів або інших документів;
- ліцензійні угоди на програмне забезпечення мають бути такими, щоб організація могла бути відповідальною за ліцензування клієнтського програмного забезпечення на робочих станціях, які власноруч придбані персоналом чи користувачами зовнішньої сторони;
- усі елементи обладнання, які містять носії пам’яті, має бути перевірено для забезпечення того, що ліцензійне програмне забезпечення було видалено чи безпечним чином перезаписано до вилучення або повторного використання.

Додаток 8

ТЕХНІЧНІ ВИМОГИ НА ЛІЦЕНЗОВАНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ ТИПОВОГО РОБОЧОГО МІСЦЯ ПРАЦІВНИКА МІСЬКОЇ РАДИ

ТЕХНІЧНЕ ЗАВДАННЯ

Класифікатор та його код відповідно до Державного класифікатору продукції та послуг:

ДК 021:2015: 48900000-7: Пакети програмного забезпечення різного призначення та різні комп’ютерні системи

Зміст

Перелік нормативних документів
Цей документ розроблений на підставі наступних нормативних документів:

1. Постанова КМУ № 1433 від 30 грудня 2021 р. “Про затвердження переліку видів продукції, торгівля якими здійснюється виключно на організованих товарних ринках”.
2. Перелік програмного забезпечення та загальні вимоги до ліцензування програмного забезпечення типового робочого місця працівника Баштанської міської ради.

Якісні та кількісні характеристики

з/п	Перелік
1	Постачання ліцензій та впровадження пакетів програмного забезпечення типового робочого місця працівника управління для роботи на 12 автоматизованих робочих місцях закладу у складі: ● Microsoft Windows 11 Professional 64-bit ● Microsoft Office 2021

Опис та основні вимоги до предмету закупівлі
Програмне забезпечення типового робочого місця працівника міської ради призначено для комплексної автоматизації основної діяльності управління і дозволяє організувати оперативний і ефективний доступ до інформації про працівників при забезпеченні необхідного рівня захисту інформації.

Спеціальне (прикладне) програмне забезпечення для РЛ повинно мати діючий експертний висновок про відповідність до вимог технічного та криптографічного захисту інформації від Державної служби спеціального зв'язку та захисту інформаціїПрограмне забезпечення, яке буде закуплене в рамках даної процедури закупівлі, повинно забезпечити комплексну автоматизацію основної діяльності міської ради і дозволити організувати оперативний і ефективний доступ до інформації про працівників при забезпеченні необхідного рівня захисту інформації із функціональними можливостями відповідно до вимог розділу «Технічна специфікація».

Гарантійні зобов'язання
Виробник (виконавець) забезпечує гарантію та термін підтримки продукту та його оновлення терміном не менше одного року.

Перелік робіт по впровадженню програмного забезпечення
Якщо вимагається встановлення програмного забезпечення на технічних засобах управління, то перелік робіт виконується відповідно до плану нижче:

1. Створення і погодження плану-графіку робіт з впровадження програмного забезпечення в закладі.
2. Впровадження програмного забезпечення відповідно до затвердженого плану-графіку робіт.
3. Проведення навчання з використання програмного забезпечення.
4. Виконання приймального тестування та інших приймально-передавальних робіт.

Вимоги до договору
Договором про закупівлю програмного забезпечення повинне бути передбачено:

- забезпечення продавцем комплектності поставки програмного продукту, зазначений у специфікації, яка додається до договору;
- встановлення у разі потреби програмного забезпечення продавцем на технічних засобах покупця;
- надання продавцем гарантійних зобов'язань;
- визначення строків та умов технічної підтримки програмного забезпечення.

Специфікація на поставку програмного забезпечення, яка додається до договору, повинна передбачати наявність:

- електронного носія інформації з примірником програмного забезпечення, до якого у разі

потреби додаються засоби для його встановлення на технічних засобах покупця;
- програмної та експлуатаційної документації на програмне забезпечення;
- ліцензії або іншого документа, що підтверджує правомірність використання програмного забезпечення.

Умови використання програмного забезпечення повинні передбачати, що строком ліцензії на використання програмного продукту є строк чинності виключних майнових прав інтелектуальної власності на відповідне програмне забезпечення.

У договорі про надання технічної підтримки програмного забезпечення повинне бути передбачено:

- перелік послуг з технічної підтримки програмного забезпечення з обґрунтуванням кошторисної вартості надання кожної з таких послуг;
- строки та порядок надання послуг;
- перелік випадків (обставин), настання яких є підставою для надання послуг на вимогу міської ради;
- перелік послуг (у разі наявності), які надаються безоплатно.

Вимоги до учасників
Учасник в складі тендерної пропозиції повинен надати документи щодо підтвердження відповідності кваліфікаційним критеріям:

1. Довідку (складену в довільній формі) щодо наявності обладнання та іншої матеріально-технічної бази, необхідних для виконання зобов'язань по договору, завірена підписом уповноваженої особи Учасника.

2. Довідку (складену в довільній формі) про наявність документально підтвердженого досвіду виконання аналогічного договору, завірена підписом уповноваженої особи Учасника.

3. Довідку (складену в довільній формі), що підтверджує наявність в учасника торгів працівників відповідної кваліфікації, яких учасник планує залучати до виконання умов договору із зазначенням: ПІБ, освіти, стажу/досвіду роботи та даних про сертифікати, дипломи, тощо.

4. Учасник має бути розробником програмного забезпечення, або бути представником, з правом поширення, що підтверджується відповідними документами (надати авторські сертифікати або свідоцтва, або сертифікати дилера/представника, або авторський договір (договори), тощо).

5. Учасник надає у складі тендерної пропозиції гарантійний лист про відповідність запропонованих послуг технічним вимогам.

6. Учасник відповідає за зміст своєї тендерної пропозиції, та повинен у складі тендерної пропозиції надати інформаційну довідку в довільній формі щодо не застосування до нього (учасника) санкцій відповідно до чинного законодавства України у даній сфері, в тому числі, але не виключно:

- Закону України «Про санкції» від 14.08.2014 № 1644-VII;

- Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» від 14.10.2014 № 1702-VII;

- Указу Президента України від 15.05.2017 № 133/2017; - Рішення РНБО України «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» від 15.05.2017;

- Постанови Кабінету Міністрів від 07.11.2014 № 595 «Деякі питання фінансування бюджетних установ, здійснення соціальних виплат населенню та надання фінансової підтримки окремим підприємствам і організаціям Донецької та Луганської областей, а також інших платежів з рахунків, відкритих в органах Казначейства»;

- Постанови Кабінету Міністрів від 16.12.2015 № 1035 «Про обмеження поставок окремих товарів (робіт, послуг) з тимчасово окупованої території на іншу територію України та/або з іншої території України на тимчасово окуповану територію»;

- Постанови Кабінету Міністрів України від 30.12.2015 № 1147 «Про заборону ввезення на митну територію України товарів, що походять з Російської Федерації».