ЗАТВЕРДЖЕНО
Наказом № 02-3 Голови
Громадської організації
«ОСВІТНІЙ КОМПАС»
від «10» січня 2026 року

ПОЛІТИКА ЦИФРОВОЇ БЕЗПЕКИ ТА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

м. Чернігів – 2026 рік

ЗМІСТ

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Ця Політика визначає основні принципи, правила та процедури забезпечення цифрової безпеки, захисту персональних даних та безпечного управління інформацією у діяльності Громадської організації «ОСВІТНІЙ КОМПАС» з урахуванням її освітньої, просвітницької, соціальної, програмної, організаційної та партнерської діяльності.

1.2. Інформаційна безпека розглядається Організацією як невід'ємна частина її діяльності, що впливає на довіру бенефіціарів, партнерів і донорів, якість реалізації проєктів, а також на дотримання прав і свобод осіб, персональні дані яких обробляються.

1.3. Політика базується на вимогах законодавства України у сфері захисту інформації та персональних даних, а також на загальновизнаних міжнародних підходах і практиках, включаючи принципи Загального регламенту захисту даних (GDPR), у частині, що може бути застосована до діяльності Організації.

1.4. Ця Політика є обов'язковою для виконання всіма особами, які залучені до діяльності Організації або мають доступ до її інформаційних ресурсів, зокрема працівниками, волонтерами, консультантами, підрядниками та партнерами.

1.5. Положення цієї Політики застосовуються до всіх процесів, пов'язаних зі збором, обробкою, зберіганням, передачею та видаленням інформації, незалежно від форми її існування (електронна чи паперова) та способу обробки.

1.6. Кожен член команди несе персональну відповідальність за дотримання вимог цієї Політики у межах своєї діяльності та зобов'язаний негайно повідомляти про будь-які випадки або ризики порушення інформаційної безпеки.

1.7. Політика підлягає періодичному перегляду та оновленню у разі змін у законодавстві, діяльності Організації, появи нових ризиків або за результатами практичного застосування її положень.

2. МЕТА ПОЛІТИКИ

2.1. Метою цієї Політики є створення в Організації ефективної системи інформаційної безпеки, яка забезпечує належний захист інформаційних ресурсів, цифрової інфраструктури та персональних даних у процесі здійснення діяльності Організації.

2.2. Політика спрямована на:

2.2.1. забезпечення захисту персональних даних бенефіціарів, членів команди, партнерів та інших осіб від несанкціонованого доступу, втрати, розголошення або знищення;

2.2.2. мінімізацію ризиків, пов'язаних із використанням електронних систем, мобільних пристроїв та цифрових сервісів;

2.2.3. встановлення чітких і єдиних правил роботи з інформацією для всіх осіб, залучених до діяльності Організації;

2.2.4. забезпечення безперервності діяльності Організації шляхом запобігання інцидентам інформаційної безпеки або мінімізації їх наслідків;

2.2.5. формування культури відповідального та етичного поводження з інформацією, зокрема у роботі з даними вразливих категорій осіб.

2.3. Особлива увага в межах цієї Політики приділяється захисту персональних даних дітей та інших вразливих груп, що передбачає підвищені стандарти конфіденційності, обмеження доступу та обробку таких даних виключно у межах визначеної мети діяльності Організації.

2.4. Політика також спрямована на забезпечення відповідності діяльності Організації вимогам законодавства України у сфері захисту інформації та персональних даних, а також вимогам партнерів і донорів щодо належного рівня цифрової безпеки.

2.5. Впровадження цієї Політики має на меті підвищення рівня довіри до діяльності Організації з боку бенефіціарів, партнерів, донорів та суспільства в цілому шляхом відповідального та системного підходу до захисту інформації.

3. СФЕРА ЗАСТОСУВАННЯ

3.1. Ця Політика поширюється на всі інформаційні ресурси, які використовуються або обробляються Організацією, незалежно від форми їх зберігання, способу обробки чи місця доступу.

3.2. Дія Політики охоплює:

3.2.1. електронні дані, включаючи документи, бази даних, листування, файли та інші цифрові матеріали;

3.2.2. інформацію, що обробляється за допомогою хмарних сервісів;

3.2.3. дані, що передаються або обговорюються через електронну пошту, месенджери та інші засоби комунікації;

3.2.4. інформацію, що зберігається на комп'ютерах, мобільних пристроях та інших носіях;

3.2.5. паперові документи, що містять персональні або інші чутливі дані.

3.3. Політика застосовується до всіх осіб, які мають доступ до інформаційних ресурсів Організації, а саме:

3.3.1. членів команди (працівників, консультантів, залучених експертів);

3.3.2. волонтерів та стажерів;

3.3.3. підрядників, партнерів та інших третіх осіб, які отримують доступ до інформації в межах співпраці з Організацією.

3.4. Положення цієї Політики поширюються також на процеси організації та проведення освітніх програм, навчальних курсів, тренінгів, сертифікаційних програм, просвітницьких заходів, конкурсів, менторських програм, дослідницьких ініціатив та інших форм статутної діяльності Організації.

3.5. Дія Політики поширюється як на використання службового обладнання, так і на особисті пристрої, які застосовуються для виконання завдань Організації, у тому числі у форматі віддаленої роботи.

3.6. Особи, які отримують доступ до інформаційних ресурсів Організації, зобов'язані дотримуватися вимог цієї Політики незалежно від місця виконання роботи, способу доступу до даних або тривалості залучення до діяльності Організації.

3.7. Надання доступу до інформації третім особам здійснюється виключно за умови наявності обґрунтованої необхідності та в межах, необхідних для виконання відповідних завдань, із дотриманням принципу мінімально необхідного доступу.

3.8. Організація залишає за собою право обмежувати, змінювати або припиняти доступ до інформаційних ресурсів у разі порушення вимог цієї Політики або виникнення ризиків для інформаційної безпеки.

4. ОСНОВНІ ТЕРМІНИ ТА ВИЗНАЧЕННЯ

4.1. У цій Політиці терміни вживаються у такому значенні:

4.1.1. **Персональні дані** – будь-яка інформація, що прямо або опосередковано стосується фізичної особи, яка ідентифікована або може бути ідентифікована.

4.1.2. **Чутливі персональні дані** – персональні дані, обробка яких може створювати підвищений ризик для прав і свобод особи, зокрема дані про дітей, стан здоров'я, соціальний статус, належність до вразливих груп, а також інша інформація, що потребує підвищеного рівня захисту.

4.1.3. **Обробка даних** – будь-яка дія або сукупність дій, що здійснюються з даними, включаючи збір, запис, зберігання, використання, передача, зміна, видалення або знищення.

4.1.4. **Інформаційні ресурси** – будь-яка інформація та засоби її обробки, що використовуються в діяльності Організації, включаючи документи, бази даних, електронні системи, хмарні сервіси та носії інформації.

4.1.5. **Доступ до інформації** – право або можливість ознайомлення з інформацією, її використання, обробки або зміни.

4.1.6. **Інцидент інформаційної безпеки** – будь-яка подія або сукупність подій, що призводить або може призвести до порушення конфіденційності, цілісності чи доступності інформації, зокрема витік даних, несанкціонований доступ, втрата пристрою або облікового запису.

4.1.7. **Несанкціонований доступ** – доступ до інформації або інформаційних систем без відповідного дозволу або з перевищенням наданих повноважень.
4.1.8. **Конфіденційна інформація** – інформація, доступ до якої обмежено Організацією або законодавством, зокрема персональні дані, внутрішні документи, інформація про бенефіціарів, партнерів та діяльність Організації.
4.1.9. **Рівень доступу** – обсяг прав, який надається особі для роботи з інформаційними ресурсами Організації відповідно до її ролі та функцій.

5. ПРИНЦИПИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

5.1.Організація забезпечує інформаційну безпеку на основі поєднання правових, організаційних та технічних заходів, із урахуванням масштабу діяльності та характеру оброблюваних даних.
5.2.Основні принципи:
5.2.1. **Мінімально необхідний доступ.** Доступ до інформаційних ресурсів надається виключно в обсязі, необхідному для виконання конкретних завдань. Кожна особа має доступ лише до тих даних, які їй необхідні для роботи.
5.2.2. **Мінімізація даних.** Організація збирає та обробляє лише ті персональні дані, які є необхідними для досягнення визначеної мети, та не допускає надмірного накопичення інформації.
5.2.3. **Конфіденційність.** Будь-яка інформація, що містить персональні або внутрішні дані, підлягає захисту від несанкціонованого доступу, розголошення або використання.
5.2.4. **Цілісність та збереження даних.** Організація забезпечує точність, повноту та збереження інформації, а також вживає заходів для запобігання її втраті або пошкодженню.
5.2.5. **Відповідальність.** Кожен член команди несе персональну відповідальність за безпечне використання інформаційних ресурсів та дотримання вимог цієї Політики.
5.2.6. **Своєчасне реагування.** У разі виникнення інцидентів інформаційної безпеки або підозри на них, Організація забезпечує оперативне реагування з метою мінімізації можливих наслідків.
5.2.7. **Захист вразливих категорій.** Обробка персональних даних дітей, осіб поважного віку та інших вразливих груп здійснюється з підвищеним рівнем обережності, із додатковими обмеженнями доступу та контролем використання таких даних.
5.2.8. **Безпечне використання цифрових інструментів.** Усі електронні системи, сервіси та засоби комунікації використовуються з дотриманням правил безпеки, встановлених цією Політикою.
5.2.9. **Розумна достатність.** Організація застосовує такі заходи безпеки, які є достатніми для захисту інформації, водночас уникаючи надмірно складних процедур, що не застосовуються на практиці.

6. КАТЕГОРІЇ ІНФОРМАЦІЇ ТА ПЕРСОНАЛЬНИХ ДАНИХ

6.1.З метою забезпечення належного рівня цифрової безпеки, захисту прав і законних інтересів бенефіціарів, партнерів, донорів, членів команди та інших осіб, Організація здійснює системну класифікацію інформації та персональних даних, що обробляються в межах її діяльності.
6.2.Класифікація інформації здійснюється залежно від характеру даних, рівня їх чутливості, цілей обробки, потенційних ризиків у разі неправомірного доступу, втрати, пошкодження або розголошення, правових та етичних вимог до захисту відповідної інформації.
6.3.Основні категорії інформації, що обробляються Організацією:
6.3.1. **Публічна інформація.**
6.3.1.1.До публічної інформації належать відомості, поширення яких не створює ризиків для прав осіб, діяльності Організації або її партнерів, та які можуть бути відкрито використані у межах інформаційної, освітньої, комунікаційної або звітної діяльності.
6.3.1.2.До такої інформації, зокрема, належать: загальна інформація про місію, напрями діяльності та програми Організації; відкриті звіти; офіційні публічні оголошення; матеріали про відкриті заходи, інформаційні кампанії; комунікаційні та презентаційні матеріали; публічні сторінки у соціальних мережах; матеріали, спеціально підготовлені для широкого розповсюдження.
6.3.2. **Внутрішня організаційна інформація.**

6.3.2.1. До цієї категорії належать дані, що використовуються для внутрішньої діяльності Організації та не призначені для вільного публічного доступу, зокрема: внутрішні плани та стратегії; проєктна документація; внутрішнє листування; операційні таблиці; контактні бази команди; робочі графіки; адміністративні документи; матеріали моніторингу; внутрішні інструкції; документи щодо управління програмами.

6.3.3. **Персональні дані учасників, бенефіціарів та заявників.**

6.3.3.1. До цієї категорії належать персональні дані осіб, які взаємодіють з Організацією через участь у програмах, освітніх заходах, реєстраціях, консультаціях чи інших активностях, зокрема: прізвище, ім'я, по батькові; контактний номер телефону; адреса електронної пошти; місце проживання або населений пункт; дата народження; місце навчання або роботи; статус учасника (учень, студент, педагог, ветеран, представник громади тощо); реєстраційні анкети; мотиваційні форми; участь у заходах; відвідуваність; оцінювання; відгуки; дані щодо навчальних досягнень або участі.

6.3.4. **Чутливі персональні дані.**

6.3.4.1. До цієї категорії належать персональні дані, обробка яких потребує підвищеного рівня захисту у зв'язку з потенційними ризиками для прав, безпеки, приватності, гідності або соціального становища особи.

6.3.4.2. До чутливих персональних даних, зокрема, належать: дані про дітей; дані про ветеранів та членів їхніх сімей; дані про осіб поважного віку; інформація про соціальний статус; інформація про складні життєві обставини; відомості про належність до вразливих категорій; письмові згоди на обробку персональних даних, фото- та відеоматеріали, що дозволяють ідентифікацію особи; інші відомості, що можуть створювати підвищені ризики у разі неправомірного використання, поширення або втрати.

6.3.5. **Дані партнерів, підрядників та контактних осіб.**

6.3.5.1. До цієї категорії належать дані, необхідні для забезпечення взаємодії Організації з партнерами, підрядниками, донорами, експертами та іншими контрагентами.

6.3.5.2. До таких даних належать: контактні дані представників партнерських організацій; службове листування; партнерські угоди; договори; офіційні листи; комунікаційні записи; документи, пов'язані зі співпрацею; інші відомості, необхідні для реалізації партнерських, адміністративних або проєктних завдань.

6.3.6. **Фінансова та бухгалтерська інформація.**

6.3.6.1. До цієї категорії належать документи та дані, пов'язані з фінансовою, бухгалтерською, грантовою та юридичною діяльністю Організації.

6.3.6.2. До такої інформації належать: договори; акти; рахунки; банківські документи; грантова документація; бюджетні плани; кошториси; фінансові звіти; бухгалтерські документи; податкові документи; юридичні матеріали, пов'язані з фінансовими процесами.

6.3.7. **Освітні, навчальні та сертифікаційні дані.**

6.3.7.1. До цієї категорії належать дані, що формуються або використовуються у процесі реалізації освітніх, навчальних, тренінгових та сертифікаційних програм Організації.

6.3.7.2. До таких даних належать: списки учасників програм; результати навчання; інформація щодо проходження курсів; сертифікаційні реєстри; освітні матеріали; документація щодо навчальних програм; база виданих сертифікатів; інші дані, пов'язані з реалізацією освітніх напрямів діяльності Організації.

7. РІВНІ ЗАХИСТУ ДАНИХ

7.1. Залежно від категорії інформації Організація встановлює три базові рівні захисту:

7.1.1. **Низький рівень захисту.** Поширюється на публічну інформацію, яка може використовуватися відкрито без істотних ризиків.

7.1.2. **Середній рівень захисту**. Поширюється на внутрішню організаційну інформацію та стандартні персональні дані.

7.1.3. **Високий рівень захисту**. Поширюється на: чутливі персональні дані; фінансову та бухгалтерську інформацію.

7.2. Визначений рівень захисту відповідної категорії інформації є обов'язковою основою для встановлення порядку її обробки, використання, зберігання та контролю в межах діяльності Організації.
7.3. Рівень захисту даних визначає: порядок надання, обмеження та припинення доступу до інформації; допустимі способи зберігання даних, у тому числі цифрового, хмарного, паперового або архівного; правила внутрішньої та зовнішньої передачі інформації; необхідні технічні заходи безпеки; строки зберігання відповідних категорій даних; порядок архівування, видалення або знеособлення інформації; вимоги до внутрішнього контролю, моніторингу та періодичного перегляду безпеки.
7.4. Організація забезпечує застосування відповідного рівня захисту на всіх етапах життєвого циклу даних – від збору до видалення або архівування.
7.5. Організація здійснює періодичний перегляд встановлених рівнів захисту даних з метою забезпечення їх актуальності та відповідності фактичним ризикам.
7.6. Перегляд рівнів захисту здійснюється, зокрема, у разі: зміни характеру або масштабів діяльності Організації; запуску нових програм, проєктів або сервісів; появи нових категорій інформації чи персональних даних; впровадження нових цифрових інструментів; виявлення нових ризиків інформаційної безпеки; змін у законодавстві України; змін у вимогах партнерів, донорів або регуляторних стандартів.
7.7. За результатами перегляду Організація може: змінювати рівень захисту окремих категорій даних; впроваджувати додаткові обмеження; посилювати технічні або організаційні заходи; оновлювати внутрішні процедури.
7.8. Для персональних даних, що стосуються: дітей; ветеранів та членів їхніх сімей; осіб поважного віку; інших соціально вразливих категорій, Організація застосовує посилений режим захисту незалежно від базового рівня класифікації.
7.9. Посилений режим передбачає: додаткове обмеження кола осіб, які мають доступ; посилені вимоги до зберігання; окремі правила передачі; додатковий контроль за використанням фото- та відеоматеріалів; спеціальні вимоги до отримання, документування та зберігання згоди; мінімізацію збору та передачі інформації; пріоритетний захист приватності, безпеки та гідності відповідних осіб.
7.10. У разі обробки таких даних Організація забезпечує застосування додаткових технічних, організаційних та етичних заходів безпеки, спрямованих на недопущення будь-якого неправомірного використання або розголошення.

8. УПРАВЛІННЯ ДОСТУПОМ ДО ІНФОРМАЦІЙНИХ РЕСУРСІВ

8.1. Положення цього розділу поширюються на доступ до: корпоративної та робочої електронної пошти; Google Workspace; Google Drive; Google Forms; Google Sheets; Google Docs; внутрішніх баз даних; CRM або реєстраційних систем; бухгалтерських ресурсів; фінансової документації; месенджерів; мобільних пристроїв; ноутбуків; соціальних мереж Організації; фото- та відеосховищ; паперових архівів; інших інформаційних ресурсів Організації.
8.2. Доступ до інформаційних ресурсів надається виключно відповідно до функціональної ролі особи в межах діяльності Організації.
8.3. До ролей можуть належати: керівник; менеджер проєкту; координатор; бухгалтер; юрист; тренер; консультант; адміністратор; комунікаційний фахівець; волонтер; підрядник; інші залучені особи.
8.4. Для кожної ролі визначається допустимий обсяг доступу з урахуванням: службових обов'язків; проєктної необхідності; категорій даних; рівня чутливості інформації; тривалості співпраці.
8.5. Надання доступу здійснюється виключно за наявності обґрунтованої операційної потреби.
8.6. Перед наданням доступу особа повинна: бути ознайомлена з цією Політикою; пройти базовий інструктаж; погодитися з вимогами інформаційної безпеки; отримати лише той обсяг доступу, який є необхідним.
8.7. Надання доступу до: персональних даних; чутливих персональних даних; фінансових документів; грантової документації; баз учасників; Google Drive; адміністрування соціальних мереж здійснюється за погодженням керівника або відповідальної особи.

8.8. У межах освітніх, навчальних та сертифікаційних програм Організація забезпечує диференційований доступ до реєстраційних, навчальних, сертифікаційних та аналітичних даних залежно від ролі працівника, координатора, тренера, адміністратора програми або іншої уповноваженої особи.

8.9. Особи, які отримали доступ до інформаційних ресурсів Організації, зобов'язані: використовувати доступ виключно в межах службових або проєктних функцій; не передавати доступ третім особам; не використовувати ресурси в особистих цілях без дозволу; не створювати несанкціоновані копії; дотримуватись вимог конфіденційності; забезпечувати безпечне використання пристроїв.

8.10. Організація здійснює періодичний перегляд актуальності доступів.

8.11. Перегляд проводиться: при зміні ролі; при зміні функцій; після завершення проєкту; після завершення співпраці; у разі інциденту; у межах внутрішнього контролю.

8.12. За результатами перегляду Організація може: обмежити доступ; змінити рівень доступу; припинити доступ; змінити паролі; оновити цифрові налаштування.

8.13. У разі завершення співпраці, зміни функціоналу або виникнення ризиків доступ припиняється без невиправданої затримки.

8.14. Припинення доступу може включати: блокування акаунтів; видалення доступів; відкликання прав редагування; зміну паролів; припинення доступу до месенджерів; припинення доступу до соціальних мереж; перевірку копій даних; архівування або повернення документів.

8.15. Організація може забезпечувати ведення внутрішнього реєстру доступів, що містить: ПІБ особи; роль; ресурси, до яких надано доступ; рівень доступу; дату надання; дату перегляду; дату припинення.

9. ВИКОРИСТАННЯ ЦИФРОВИХ ІНСТРУМЕНТІВ, ЕЛЕКТРОННОЇ ПОШТИ ТА КОМУНІКАЦІЙНИХ ЗАСОБІВ

9.1. Використання цифрових ресурсів Організації здійснюється виключно відповідно до вимог цієї Політики, принципів інформаційної безпеки, захисту персональних даних, конфіденційності, розумної достатності та практичної доцільності.

9.2. До цифрових ресурсів Організації належать, зокрема: корпоративна або погоджена робоча електронна пошта; Google Workspace; Google Drive; Google Forms; Google Sheets; Google Docs; месенджери; мобільні телефони; ноутбуки; стаціонарні ПК; сервіси відеозв'язку; соціальні мережі; CRM або внутрішні бази; сервіси фінансового адміністрування; фото- та відеосховища; інші погоджені цифрові платформи.

9.3. **Використання електронної пошти.**

9.3.1. Електронна пошта є одним із базових офіційних каналів комунікації Організації.

9.3.2. Для роботи з: персональними даними; внутрішньою документацією; фінансовими матеріалами; грантовими документами; юридичними матеріалами; партнерським листуванням використовуються виключно погоджені робочі або корпоративні електронні адреси.

9.3.3. Особи, які використовують електронну пошту, зобов'язані: перевіряти адресатів; перевіряти вкладення; не відкривати підозрілі листи; використовувати складні паролі; застосовувати двофакторну автентифікацію; своєчасно повідомляти про підозри на фішинг або компрометацію.

9.3.4. Забороняється: передавати доступи до пошти; використовувати непогоджені поштові сервіси для критичних даних; поширювати чутливі дані без належного захисту; використовувати електронну пошту з порушенням вимог конфіденційності.

9.4. **Використання Google Workspace, Google Drive, Google Forms та Google Sheets.**

9.4.1. Google Workspace є одним із основних цифрових середовищ діяльності Організації.

9.4.2. Google Forms можуть використовуватися для: реєстрації учасників; збору анкет; заявок; згод; моніторингу; оцінювання; освітніх програм; сертифікації; звітності.

9.4.3. Google Drive, Google Sheets та Google Docs використовуються для: зберігання документів; адміністрування програм; ведення баз даних; фінансової документації; аналітики; внутрішньої комунікації; архівування.

9.4.4. Організація забезпечує: контроль доступів; рольове розмежування; обмеження поширення; перегляд прав доступу; резервне копіювання критично важливих матеріалів; архівування; контроль обробки чутливих даних.

9.4.5. Забороняється: відкритий доступ без потреби; використання сторонніх особистих акаунтів без погодження; створення несанкціонованих копій; зберігання чутливих даних без належного рівня захисту.

9.5.**Використання месенджерів.**

9.5.1. Месенджери використовуються переважно для оперативної робочої координації.

9.5.2. Допускається використання месенджерів для: внутрішньої координації; організаційної комунікації; оперативних повідомлень; комунікації в межах програм за умови дотримання вимог безпеки.

9.5.3. Забороняється: використовувати месенджери як основне сховище даних; зберігати у месенджерах бази персональних даних; передавати чутливу інформацію без потреби; використовувати месенджери всупереч вимогам конфіденційності.

9.6.**Використання мобільних телефонів, ноутбуків, стаціонарних ПК та інших пристроїв.**

9.6.1. Усі пристрої, що використовуються для роботи, повинні бути захищені: паролями; блокуванням екрана; базовими технічними заходами безпеки; оновленнями систем.

9.6.2. У разі втрати, компрометації або підозри на несанкціонований доступ особа зобов’язана негайно повідомити відповідальну особу.

9.6.3. Особисті пристрої можуть використовуватися лише за умови дотримання вимог цієї Політики.

9.7.**Фото-, відеоматеріали та медіадані.**

9.7.1. Фото- та відеоматеріали, що містять зображення учасників програм, бенефіціарів або членів команди, можуть становити персональні дані.

9.7.2. Використання таких матеріалів здійснюється: у межах визначеної мети; за наявності належної правової підстави; з урахуванням згоди; з особливою обережністю щодо дітей та інших вразливих категорій.

9.7.3. Організація забезпечує: контроль доступу; безпечне зберігання; контроль публікацій; захист прав осіб.

9.8.**Соціальні мережі та публічні цифрові платформи.**

9.8.1. Офіційні сторінки та цифрові платформи Організації адмініструються визначеними особами.

9.8.2. Організація забезпечує: контроль доступу; безпечне зберігання паролів; двофакторну автентифікацію; контроль публікацій; захист репутаційних інтересів.

9.8.3. Забороняється: публікація чутливих даних без належних підстав; використання офіційних ресурсів у приватних цілях; поширення інформації з порушенням прав суб’єктів даних.

9.9.**Перегляд цифрових практик.**

9.9.1. Організація здійснює періодичний перегляд використання цифрових інструментів з урахуванням: нових ризиків; змін у діяльності; впровадження нових сервісів; законодавчих змін; партнерських або донорських вимог.

10. РЕАГУВАННЯ НА ІНЦИДЕНТИ ЦИФРОВОЇ БЕЗПЕКИ

10.1. Інцидентом цифрової безпеки вважається будь-яка подія, дія, бездіяльність або обставина, що створює або може створити загрозу: конфіденційності; цілісності; доступності інформації; безпеці цифрових ресурсів; правам суб’єктів персональних даних; стабільності діяльності Організації.

10.2. До інцидентів цифрової безпеки можуть належати, зокрема: несанкціонований доступ до акаунтів; компрометація електронної пошти; злам Google Drive; несанкціонований доступ до Google Forms, Sheets або інших цифрових систем; витік персональних даних; помилкове надсилання конфіденційної інформації; фішингові атаки; зараження шкідливим програмним забезпеченням; втрата або крадіжка пристрою; порушення правил доступу; несанкціоноване використання фото- чи відеоматеріалів; втручання у фінансову документацію; порушення вимог щодо чутливих категорій даних.

10.3. Кожна особа, яка виявила, підозрює або стала свідком потенційного інциденту цифрової безпеки, зобов'язана негайно повідомити: керівника Організації; відповідальну особу; адміністратора цифрового ресурсу (за наявності).
10.4. Повідомлення здійснюється без невиправданої затримки, бажано одразу після виявлення.
10.5. У разі виявлення інциденту можуть здійснюватися такі першочергові дії: зміна паролів; вихід із скомпрометованих сесій; блокування акаунтів; обмеження доступів; припинення роботи з ураженим пристроєм; відкликання доступу до файлів; ізоляція цифрового ресурсу; фіксація обставин події; повідомлення залучених сторін.
10.6. Організація може забезпечувати ведення журналу інцидентів цифрової безпеки.
10.7. Після первинного реагування Організація здійснює оцінку: масштабу інциденту; потенційних наслідків; ризиків для суб'єктів даних; впливу на діяльність; фінансових наслідків; репутаційних ризиків; необхідності зовнішнього повідомлення.
10.8. У разі інциденту, що стосується: дітей, інших соціально вразливих категорій Організація застосовує посилені заходи, зокрема: негайне обмеження доступу; підвищений контроль; окрему оцінку ризиків; пріоритетний захист постраждалих осіб; спеціальний порядок подальших дій.
10.9. У разі суттєвих інцидентів Організація може повідомляти: суб'єктів персональних даних; партнерів; донорів; підрядників; інші залучені сторони, якщо це є необхідним для мінімізації шкоди, виконання зобов'язань або дотримання законодавства.
10.10. Після локалізації інциденту Організація забезпечує: відновлення доступу; зміну паролів; оновлення налаштувань безпеки; коригування доступів; перегляд процедур; додаткове навчання; технічне посилення захисту.
10.11. Організація здійснює аналіз причин інциденту з метою: недопущення повторення; усунення системних недоліків; посилення політик; вдосконалення внутрішніх процедур; підвищення рівня цифрової обізнаності.
10.12. Особи, які добросовісно повідомляють про інциденти або потенційні ризики, не повинні зазнавати негативних наслідків лише через факт такого повідомлення, якщо їхні дії не були умисним порушенням.

11. ЗБЕРІГАННЯ, АРХІВУВАННЯ, ВИДАЛЕННЯ ТА ЗНЕОСОБЛЕННЯ ДАНИХ

11.1. Дані зберігаються виключно у визначених Організацією середовищах з урахуванням: категорії інформації; рівня її чутливості; правових вимог; технічної доцільності; організаційної безпеки.
11.2. До основних середовищ зберігання можуть належати: Google Drive; Google Workspace; захищені електронні таблиці; корпоративна електронна пошта; фінансові сервіси; паперові архіви; внутрішні реєстри; CRM-системи; сертифікаційні бази; інші погоджені середовища.
11.3. Організація забезпечує: обмеження доступу; контроль поширення; систематизацію; резервне копіювання критичних матеріалів; захист від випадкової втрати; контроль цілісності даних.
11.4. Паперові носії інформації, що містять персональні дані бенефіціарів, заявників, учасників програм, а також чутливі персональні дані, зокрема дані дітей, ветеранів, осіб поважного віку, правові документи, кейс-матеріали та інші документи підвищеного рівня чутливості, зберігаються у спеціально визначених фізично захищених місцях (сейфах, шафах із обмеженим доступом або інших захищених приміщеннях), доступ до яких мають виключно уповноважені особи відповідно до внутрішніх правил Організації.
11.5. Строки зберігання визначаються залежно від: вимог законодавства; грантових умов; фінансової звітності; цілей програм; освітніх або сертифікаційних процесів; потреб моніторингу; необхідності захисту прав осіб.
11.6. Освітні, навчальні та сертифікаційні реєстри, бази учасників програм, результати проходження навчання та документи щодо освітньої діяльності зберігаються у визначених Організацією захищених середовищах відповідно до строків, необхідних для реалізації програм, сертифікації, звітності, моніторингу та виконання статутних або партнерських зобов'язань.
11.7. Організація не допускає зберігання даних довше, ніж це є обґрунтовано необхідним.

11.8. Дані, які більше не використовуються в активній операційній діяльності, але підлягають збереженню з правових, фінансових, звітних або програмних причин, переводяться до архівного режиму.
11.9. Архівування передбачає: обмеження доступу; структурування; контрольоване зберігання; мінімізацію випадкового використання; можливість відновлення за потреби.
11.10. Чутливі категорії даних архівуються з підвищеним рівнем захисту.
11.11. Видалення даних здійснюється у разі: досягнення мети обробки; завершення строків зберігання; завершення проєкту; відсутності правових підстав для подальшого зберігання; відкликання згоди (у передбачених випадках); необхідності мінімізації ризиків.
11.12. Видалення має бути: контрольованим; своєчасним; безпечним; пропорційним; таким, що унеможливлює подальше неналежне використання.
11.13. У випадках, коли інформація необхідна для: аналітики; моніторингу; звітності; досліджень; програмного аналізу, але не потребує ідентифікації конкретної особи, Організація може застосовувати знеособлення даних.
11.14. Знеособлення передбачає: видалення ідентифікаційних ознак; мінімізацію ризику повторної ідентифікації; контроль доступу; використання виключно в дозволених цілях.
11.15. Організація забезпечує резервне копіювання критично важливої інформації в межах практичної доцільності.
11.16. До критично важливих даних можуть належати: фінансова документація; грантові матеріали; правові документи; ключові реєстри; освітні сертифікаційні бази; документи стратегічного управління.
11.17. Організація здійснює періодичний перегляд: актуальності даних; строків зберігання; архівів; резервних копій; обсягів збережених персональних даних; потреби у видаленні; необхідності оновлення процедур.
11.18. Особи, які працюють із даними Організації, зобов'язані: використовувати визначені середовища зберігання; не створювати надлишкових копій; дотримуватись строків зберігання; забезпечувати належне архівування; своєчасно ініціювати видалення; дотримуватись вимог цієї Політики; діяти з урахуванням принципів конфіденційності та безпеки.

12. НАВЧАННЯ, ОБІЗНАНІСТЬ ТА ВНУТРІШНЄ ВПРОВАДЖЕННЯ ПОЛІТИКИ

12.1. Організація визнає належний рівень обізнаності членів команди одним із ключових елементів забезпечення цифрової безпеки, захисту персональних даних та ефективного практичного впровадження цієї Політики.
12.2. Організація забезпечує ознайомлення всіх осіб, які залучаються до її діяльності та отримують доступ до інформаційних ресурсів, із положеннями цієї Політики до початку виконання відповідних функцій або завдань.
12.3. До початку роботи або отримання доступу до даних кожна особа повинна: ознайомитися з Політикою; отримати базовий інструктаж; розуміти основні вимоги щодо захисту інформації; підтвердити обізнаність із внутрішніми правилами.
12.4. Первинний інструктаж охоплює, зокрема: правила роботи з персональними даними; класифікацію даних; рівні захисту; правила використання Google Workspace; безпечну роботу з електронною поштою; використання месенджерів; правила доступу; порядок реагування на інциденти; особливості роботи з чутливими категоріями даних.
12.5. Організація забезпечує періодичне оновлення знань членів команди з питань цифрової безпеки відповідно до: змін у законодавстві; розвитку програм; впровадження нових цифрових інструментів; появи нових ризиків; змін внутрішніх процедур.
12.6. Таке оновлення може здійснюватися у формі: внутрішніх нагадувань; коротких інструктажів; оновлених процедур; навчальних матеріалів; командних обговорень.
12.7. Організація забезпечує періодичне підвищення рівня цифрової грамотності, інформаційної безпеки та безпечного використання персональних даних серед членів команди, координаторів програм, тренерів, освітніх працівників та інших осіб, залучених до реалізації освітніх і просвітницьких програм.

12.8. Навчання та внутрішня комунікація з питань інформаційної безпеки повинні бути: практичними; зрозумілими; пропорційними масштабу діяльності Організації; орієнтованими на реальні ризики; такими, що можуть бути ефективно застосовані в щоденній роботі.
12.9. Організація уникає надмірно складних процедур, які не відповідають фактичним потребам її діяльності.
12.10. Організація сприяє формуванню внутрішньої культури відповідального ставлення до інформації, що передбачає: уважність до ризиків; своєчасне повідомлення про підозри; відкриту комунікацію; дотримання процедур; спільну відповідальність за безпеку.
12.11. Організація може забезпечувати фіксацію: ознайомлення з Політикою; проходження інструктажів; оновлення знань; прийняття внутрішніх правил.
12.12. У разі оновлення цієї Політики або окремих процедур Організація забезпечує належне повторне ознайомлення членів команди з відповідними змінами.
12.13. Усі особи, які працюють в Організації або залучаються до її діяльності, зобов'язані: знати базові вимоги цієї Політики; дотримуватись внутрішніх правил; підтримувати належний рівень цифрової безпеки; діяти добросовісно при роботі з інформацією; сприяти практичному впровадженню цієї Політики у щоденній діяльності Організації.

13. КОНТРОЛЬ, МОНІТОРИНГ ТА ПЕРЕГЛЯД ПОЛІТИКИ

13.1. Організація забезпечує внутрішній контроль за дотриманням вимог цієї Політики, моніторинг практичного застосування встановлених процедур та періодичний перегляд документа з метою підтримання його актуальності, ефективності та відповідності фактичним потребам діяльності Організації.
13.2. Контроль за виконанням положень цієї Політики здійснюється керівником Організації або визначеною відповідальною особою в межах повноважень, необхідних для належного адміністрування цифрової безпеки та захисту персональних даних.
13.3. Контроль охоплює, зокрема: дотримання правил роботи з персональними даними; застосування рівнів захисту інформації; управління доступами; використання цифрових інструментів; належне зберігання, архівування та видалення даних; дотримання процедур реагування на інциденти; виконання вимог щодо чутливих категорій даних; актуальність внутрішніх інструкцій та додатків.
13.4. Організація може застосовувати: періодичний перегляд доступів; перевірку використання цифрових ресурсів; аналіз інцидентів; перегляд актуальності збережених даних; контроль за дотриманням строків зберігання; оцінку практичного впровадження внутрішніх процедур; оновлення карти даних; перевірку відповідності вимогам партнерів і донорів.
13.5. Політика підлягає перегляду у разі: змін у законодавстві; запуску нових програм; зміни напрямів діяльності; впровадження нових цифрових інструментів; появи нових категорій даних; зміни ризиків; суттєвих інцидентів; змін у вимогах партнерів або донорів.
13.6. Перегляд Політики також здійснюється періодично з метою підтримання її актуальності навіть за відсутності істотних змін.
13.7. За результатами контролю або перегляду Організація може: оновлювати окремі положення; змінювати рівні захисту; посилювати процедури; оновлювати додатки; змінювати внутрішні інструкції; впроваджувати нові механізми безпеки.
13.8. У разі виявлення порушень, прогалин або ризиків Організація забезпечує: коригування процедур; обмеження доступів; додаткове навчання; оновлення цифрових налаштувань; інші необхідні заходи.
13.9. Організація може забезпечувати ведення документації щодо: перегляду Політики; змін процедур; інцидентів; контролю доступів; проведених інструктажів; прийнятих рішень щодо безпеки.
13.10. Контроль та моніторинг здійснюються з урахуванням: масштабу Організації; обсягу діяльності; кількості членів команди; реальних ризиків; доступних ресурсів.
13.11. Організація застосовує достатній рівень контролю без створення надмірного адміністративного навантаження.

13.12. Метою контролю та перегляду є: підтримання актуальності Політики; забезпечення практичної дієвості; підвищення рівня цифрової безпеки; захист прав суб'єктів персональних даних; зміцнення інституційної спроможності Організації.

14. ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ПОЛІТИКИ

14.1. Усі особи, на яких поширюється дія цієї Політики, несуть персональну відповідальність за дотримання її вимог у межах своїх функцій, ролей та доступів.
14.2. Порушенням вимог Політики можуть вважатися, зокрема: несанкціоноване використання інформації; неналежне зберігання даних; передача доступів третім особам; порушення конфіденційності; ігнорування правил цифрової безпеки; приховування інцидентів; неналежна обробка персональних даних; порушення правил роботи з чутливими категоріями даних; використання інформаційних ресурсів усупереч визначеній меті; інші дії або бездіяльність, що створюють ризики для безпеки Організації чи прав суб'єктів даних.
14.3. Особи, які допустили порушення, можуть нести відповідальність відповідно до: внутрішніх процедур Організації; умов співпраці; трудових або цивільно-правових договорів; партнерських зобов'язань; грантових вимог; чинного законодавства України.
14.4. Залежно від характеру порушення Організація може застосовувати: усне або письмове застереження; додаткове навчання; обмеження доступу; тимчасове блокування ресурсів; перегляд повноважень; дисциплінарні заходи; припинення співпраці; повідомлення партнерів або донорів (за потреби); інші заходи відповідно до законодавства та внутрішніх процедур.
14.5. Добросовісне повідомлення про ризики, помилки або інциденти не вважається порушенням, якщо особа діяла чесно, без умислу та відповідно до внутрішніх процедур.
14.6. Організація прагне не лише до реагування на порушення, а й до формування культури відповідального, етичного та безпечного поводження з інформацією.

15. ПРИКІНЦЕВІ ПОЛОЖЕННЯ

15.1. Ця Політика вводиться в дію на підставі відповідного внутрішнього рішення Організації та є базовим внутрішнім документом, що визначає загальні організаційні підходи до цифрової безпеки, захисту персональних даних та безпечного управління інформацією.
15.2. У разі виникнення суперечностей між окремими внутрішніми процедурами, інструкціями або практиками та положеннями цієї Політики, пріоритет застосування мають положення цієї Політики, якщо інше не встановлено законодавством України.
15.3. Положення цієї Політики застосовуються у взаємозв'язку з: внутрішніми процедурами; наказами; додатками; партнерськими зобов'язаннями; грантовими вимогами; іншими внутрішніми документами Організації.
15.4. У випадках, не врегульованих цією Політикою, Організація керується: чинним законодавством України; принципами захисту прав людини; принципами конфіденційності; вимогами безпеки; етичними стандартами діяльності; принципом найкращого захисту прав суб'єктів персональних даних.
15.5. Усі структурні елементи Політики, включаючи додатки, форми, журнали, реєстри та внутрішні інструкції, формують єдину систему управління цифровою безпекою Організації.
15.6. Реалізація цієї Політики спрямована також на підтримку безпечного розвитку освітніх, просвітницьких та інноваційних напрямів діяльності Організації відповідно до її статутної мети.
15.7. Ця Політика підлягає офіційному зберіганню як внутрішній нормативний документ Організації та використовується як основа для подальшого розвитку процедур цифрової безпеки, захисту персональних даних і внутрішнього управління інформацією.

16. ПЕРЕЛІК ДОДАТКІВ ДО ПОЛІТИКИ

16.1.Невід’ємною частиною цієї Політики є додатки, що деталізують окремі практичні процедури, форми, інструкції, реєстри та внутрішні механізми реалізації вимог цифрової безпеки та захисту персональних даних у діяльності Організації.

16.2.До цієї Політики додаються:

Додаток 1. Інструкція з інформаційної безпеки для членів команди;
Додаток 2. Алгоритм реагування на інциденти цифрової безпеки;
Додаток 3. Правила надання, перегляду та припинення доступу до інформаційних ресурсів;
Додаток 4. Правила роботи з чутливими персональними даними;
Додаток 5. Форма згоди на обробку персональних даних;
Додаток 6. Форма ознайомлення з Політикою цифрової безпеки та захисту персональних даних;
Додаток 7. Журнал інцидентів цифрової безпеки;
Додаток 8. Реєстр доступів до інформаційних ресурсів.

16.3.Додатки підлягають застосуванню нарівні з основним текстом цієї Політики та можуть оновлюватися відповідно до змін у діяльності Організації, законодавстві, внутрішніх процедурах або за результатами контролю та перегляду.

ДОДАТОК 1

ІНСТРУКЦІЯ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ ЧЛЕНІВ КОМАНДИ ГРОМАДСЬКОЇ ОРГАНІЗАЦІЇ «ОСВІТНІЙ КОМПАС»

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Ця Інструкція визначає базові обов'язкові правила цифрової безпеки для всіх працівників, волонтерів, консультантів, підрядників та інших осіб, які залучені до діяльності Організації або мають доступ до її інформаційних ресурсів.
1.2. Інструкція спрямована на: захист персональних даних; збереження конфіденційної інформації; мінімізацію ризиків витоку даних; безпечне використання цифрових інструментів; запобігання інцидентам цифрової безпеки.
1.3. Кожен член команди зобов'язаний дотримуватися цієї Інструкції у щоденній діяльності.

2. ЕЛЕКТРОННА ПОШТА

2.1. Для роботи з документами, персональними даними, внутрішньою документацією та офіційною комунікацією використовуються виключно погоджені робочі електронні адреси.
2.2. Забороняється: передавати доступ до пошти іншим особам; використовувати сторонні або непогоджені акаунти для критичної інформації; відкривати підозрілі листи або вкладення; переходити за сумнівними посиланнями.
2.3. Перед надсиланням інформації необхідно перевіряти: адресу отримувача; вкладення; обсяг переданих даних; наявність чутливої інформації.

3. ПАРОЛІ ТА АВТЕНТИФІКАЦІЯ

3.1. Усі робочі акаунти повинні бути захищені надійними унікальними паролями.
3.2. Для всіх критично важливих сервісів обов'язково використовується двофакторна автентифікація (2FA).
3.3. Забороняється: передавати паролі; зберігати паролі у відкритому вигляді; використовувати однакові паролі для різних сервісів; використовувати очевидні або слабкі паролі.

4. GOOGLE DRIVE ТА ДОКУМЕНТИ

4.1. Документи Організації зберігаються виключно у визначених цифрових середовищах.
4.2. Доступ до документів надається лише відповідно до ролі та потреби.
4.3. Забороняється: створювати несанкціоновані копії; відкривати загальний доступ без погодження; зберігати чутливі дані у незахищених середовищах; використовувати особисті акаунти без дозволу.

5. МЕСЕНДЖЕРИ

5.1. Месенджери використовуються переважно для оперативної комунікації.
5.2. Забороняється: зберігати повноцінні бази персональних даних; передавати великі масиви чутливої інформації без необхідності; використовувати месенджери як основне сховище документів.
5.3. У разі передачі важливої інформації слід мінімізувати обсяг персональних даних.

6. МОБІЛЬНІ ПРИСТРОЇ ТА КОМП'ЮТЕРИ

6.1. Усі пристрої, що використовуються для роботи, повинні бути захищені: паролем; блокуванням екрана; оновленнями систем; базовими заходами безпеки.
6.2. Забороняється: залишати пристрої без нагляду з відкритим доступом; передавати робочі пристрої стороннім особам без погодження; зберігати чутливі дані без захисту.

6.3.У разі втрати пристрою необхідно негайно повідомити керівництво.

7. РОБОТА З ЧУТЛИВИМИ ДАНИМИ

7.1.Дані осіб вразливих категорій потребують підвищеного рівня захисту.
7.2.Забороняється: передавати такі дані без потреби; обговорювати їх у відкритих каналах; використовувати без належної правової підстави; поширювати фото/відео без відповідних дозволів.

8. ПІДОЗРІЛІ СИТУАЦІЇ ТА ІНЦИДЕНТИ

8.1.У разі: підозрілих листів; втрати пристрою; підозри на злам; випадкового надсилання даних; підозри на витік інформації необхідно негайно повідомити керівника або відповідальну особу.
8.2.Не допускається приховування потенційних ризиків.

9. ОСОБИСТА ВІДПОВІДАЛЬНІСТЬ

9.1.Кожен член команди несе персональну відповідальність за: безпечне використання цифрових ресурсів; захист доступів; дотримання цієї Інструкції; конфіденційність; добросовісне поводження з інформацією.

10. ЗАКЛЮЧНІ ПОЛОЖЕННЯ

10.1. Ця Інструкція є обов’язковою для всіх осіб, які мають доступ до ресурсів Організації.
10.2. Порушення Інструкції може призвести до: обмеження доступу; внутрішніх заходів реагування; перегляду повноважень; припинення співпраці; інших заходів відповідно до внутрішніх процедур Організації.

ДОДАТОК 2

АЛГОРИТМ РЕАГУВАННЯ НА ІНЦИДЕНТИ ЦИФРОВОЇ БЕЗПЕКИ ГРОМАДСЬКОЇ ОРГАНІЗАЦІЇ «ОСВІТНІЙ КОМПАС»

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Цей Алгоритм визначає обов'язковий порядок дій у разі виявлення, підозри або підтвердження інцидентів цифрової безпеки в діяльності Організації.
1.2. Метою Алгоритму є: своєчасне виявлення ризиків; мінімізація шкоди; захист персональних даних; захист чутливої інформації; локалізація інцидентів; забезпечення безперервності діяльності Організації; запобігання повторним порушенням.
1.3. Алгоритм застосовується до всіх членів команди, волонтерів, підрядників та інших осіб, які мають доступ до цифрових ресурсів Організації.

2. ЩО ВВАЖАЄТЬСЯ ІНЦИДЕНТОМ

2.1. Інцидентом цифрової безпеки можуть бути: підозра на злам акаунту; несанкціонований доступ; витік персональних даних; випадкове надсилання конфіденційної інформації; фішингові повідомлення; зараження шкідливим програмним забезпеченням; втрата або крадіжка пристрою; компрометація паролів; порушення правил доступу; несанкціоноване використання фото-, відео- або документальних матеріалів; будь-які інші події, що можуть загрожувати цифровій безпеці.

3. ЕТАП 1. ВИЯВЛЕННЯ ІНЦИДЕНТУ

3.1. Будь-яка особа, яка: виявила інцидент; підозрює інцидент; стала свідком ризикової ситуації, зобов'язана негайно розпочати процедуру реагування. Навіть потенційний ризик розглядається як підстава для реагування.

4. ЕТАП 2. НЕГАЙНЕ ПОВІДОМЛЕННЯ

4.1. Повідомлення здійснюється без зволікань, бажано протягом 1 години з моменту виявлення.
4.2. Повідомляється: Голова Організації; відповідальна особа; адміністратор ресурсу (за наявності).
4.3. Повідомлення повинно містити: короткий опис ситуації; дату і час; залучені ресурси; категорії даних; первинні відомості про ризики.

5. ЕТАП 3. ПЕРВИННІ ЗАХОДИ ЛОКАЛІЗАЦІЇ

5.1. За потреби негайно здійснюються: зміна паролів; вихід з акаунтів; блокування доступу; припинення використання пристрою; відкликання прав доступу; ізоляція пристрою; зупинка поширення даних; резервне збереження важливої інформації.

6. ЕТАП 4. ФІКСАЦІЯ І ДОКУМЕНТУВАННЯ

6.1. Відповідальна особа забезпечує документування інциденту.
6.2. Інформація вноситься до Журналу інцидентів цифрової безпеки.

7. ЕТАП 5. ОЦІНКА МАСШТАБУ ТА РИЗИКІВ

7.1. Проводиться аналіз: масштабу інциденту; ризику для персональних даних; ризику для дітей; ризику для ветеранів; ризику для осіб поважного віку; фінансових ризиків; репутаційних наслідків; донорських ризиків; правових наслідків.

8. ЕТАП 6. ПРИЙНЯТТЯ РІШЕНЬ

8.1. За результатами оцінки можуть прийматися рішення щодо: подальшого блокування; технічного відновлення; зміни правил доступу; повідомлення постраждалих осіб; повідомлення партнерів; повідомлення донорів; оновлення внутрішніх процедур; проведення додаткового навчання.

9. ЕТАП 7. ВІДНОВЛЕННЯ ТА КОРЕКЦІЯ

9.1. Організація забезпечує: відновлення роботи; оновлення налаштувань; зміну паролів; перегляд доступів; додатковий контроль; посилення технічного захисту; корекцію процедур.

10. ЕТАП 8. АНАЛІЗ І ПРОФІЛАКТИКА

10.1. Після завершення реагування проводиться: аналіз причин; оцінка системних слабких місць; оновлення політик; перегляд інструкцій; додаткове навчання; коригування внутрішніх процесів.

11. ОСОБЛИВИЙ ПОРЯДОК ДЛЯ ЧУТЛИВИХ ДАНИХ

11.1. У разі інцидентів, пов’язаних із даними: дітей та інших вразливих категорій, застосовуються: підвищений контроль; пріоритетне реагування; окремий аналіз наслідків; посилені заходи безпеки.

12. ЗАГАЛЬНІ ПРАВИЛА

12.1. Забороняється: приховувати інциденти; ігнорувати підозри; самостійно замовчувати ризики; продовжувати небезпечну роботу без погодження.
12.2. Добросовісне повідомлення про інцидент є обов’язком члена команди.

13. ВІДПОВІДАЛЬНІСТЬ

13.1. Недотримання цього Алгоритму може бути підставою для: перегляду доступів; дисциплінарних заходів; припинення співпраці; інших заходів відповідно до внутрішніх процедур Організації.

ДОДАТОК 3

ПРАВИЛА НАДАННЯ, ПЕРЕГЛЯДУ ТА ПРИПИНЕННЯ ДОСТУПУ ДО ІНФОРМАЦІЙНИХ РЕСУРСІВ ГРОМАДСЬКОЇ ОРГАНІЗАЦІЇ «ОСВІТНІЙ КОМПАС»

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Ці Правила визначають порядок надання, обмеження, перегляду та припинення доступу до інформаційних ресурсів Організації.
1.2. Метою Правил є: забезпечення безпечного доступу; захист персональних даних; мінімізація ризиків несанкціонованого використання; реалізація принципу мінімально необхідного доступу; контроль цифрових ресурсів Організації.
1.3. Правила поширюються на всіх працівників, волонтерів, консультантів, підрядників та інших осіб, які отримують доступ до ресурсів Організації.

2. РЕСУРСИ, ДО ЯКИХ МОЖЕ НАДАВАТИСЯ ДОСТУП

2.1. Доступ може надаватися до: електронної пошти; Google Workspace; Google Drive; Google Forms; Google Sheets; Google Docs; фінансових ресурсів; внутрішніх реєстрів; CRM-систем; баз персональних даних; соціальних мереж; фото- та відеосховищ; паперових архівів; інших інформаційних ресурсів Організації.

3. НАДАННЯ ДОСТУПУ

3.1. Доступ надається виключно у разі обґрунтованої потреби для виконання конкретних функцій.
3.2. Перед наданням доступу особа повинна: бути ознайомлена з Політикою; пройти базовий інструктаж; підтвердити ознайомлення; погодитися з вимогами конфіденційності; отримати лише необхідний обсяг доступу.
3.3. Надання доступу до: чутливих персональних даних; фінансових документів; грантової документації; стратегічних документів; соціальних мереж; баз даних здійснюється лише за погодженням керівника або відповідальної особи.

4. ВИКОРИСТАННЯ ДОСТУПУ

4.1. Особа, яка отримала доступ, зобов’язана: використовувати ресурси виключно в межах службових функцій; не передавати доступ іншим особам; не використовувати доступ у приватних цілях; не створювати несанкціоновані копії; забезпечувати конфіденційність; дотримуватися внутрішніх процедур безпеки.

5. ОБМЕЖЕННЯ ДОСТУПУ

5.1. Організація може обмежувати доступ: у разі зміни ролі; при завершенні проєкту; при завершенні співпраці; у разі ризику; при порушенні вимог безпеки; за результатами контролю.
5.2. Обмеження може включати: зміну прав доступу; обмеження редагування; блокування акаунтів; зміну паролів; відкликання прав адміністратора.

6. ПЕРІОДИЧНИЙ ПЕРЕГЛЯД ДОСТУПІВ

6.1. Організація здійснює регулярний перегляд доступів з метою перевірки: актуальності; необхідності; відповідності ролі; рівня ризиків; безпечності використання.
6.2. Перегляд проводиться: при кадрових змінах; після завершення проєктів; після інцидентів; під час внутрішнього контролю; у межах оновлення цифрової безпеки.

7. ПРИПИНЕННЯ ДОСТУПУ

7.1. Доступ припиняється без невиправданої затримки у разі: завершення співпраці; зміни функціоналу; звільнення; завершення договору; втрати необхідності; виявлення ризиків; порушення вимог безпеки.

7.2. Припинення доступу може включати: блокування акаунтів; зміну паролів; видалення прав; вихід із систем; перевірку копій; архівування; повернення документів.

8. ОСОБЛИВИЙ ПОРЯДОК ДЛЯ ЧУТЛИВИХ ДАНИХ

8.1. Доступ до даних: дітей; ветеранів; членів сімей ветеранів; осіб поважного віку; інших вразливих категорій надається лише визначеним особам із підвищеним контролем.

9. РЕЄСТР ДОСТУПІВ

9.1. Організація може вести внутрішній реєстр доступів, який містить: ПІБ; роль; ресурс; рівень доступу; дату надання; дату перегляду; дату припинення; примітки.

10. ЗАБОРОНИ

10.1. Забороняється: передача доступів; спільне використання акаунтів без дозволу; приховування втрати доступу; несанкціоноване копіювання; використання сторонніх ресурсів без погодження; зберігання доступів у незахищеному вигляді.

11. ВІДПОВІДАЛЬНІСТЬ

11.1. Недотримання цих Правил може бути підставою для: обмеження доступу; дисциплінарних заходів; припинення співпраці; внутрішнього перегляду повноважень; інших заходів відповідно до політик Організації.

ДОДАТОК 4

ПРАВИЛА РОБОТИ З ЧУТЛИВИМИ ПЕРСОНАЛЬНИМИ ДАНИМИ ГРОМАДСЬКОЇ ОРГАНІЗАЦІЇ «ОСВІТНІЙ КОМПАС»

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Ці Правила визначають спеціальний порядок збору, обробки, використання, передачі, зберігання, архівування та видалення чутливих персональних даних у діяльності Організації.
1.2. Метою Правил є: забезпечення підвищеного рівня захисту; захист прав, безпеки, гідності та приватності осіб; мінімізація ризиків неправомірного використання; забезпечення етичної роботи з вразливими категоріями; дотримання законодавства та внутрішніх стандартів.

2. ДО ЧУТЛИВИХ ПЕРСОНАЛЬНИХ ДАНИХ НАЛЕЖАТЬ

2.1. До цієї категорії належать, зокрема, дані щодо: дітей; ветеранів; членів сімей ветеранів; осіб поважного віку; осіб із соціальною вразливістю; осіб у складних життєвих обставинах; учасників правозахисних програм; фото- та відеоматеріали, що дозволяють ідентифікацію; письмові згоди; інші дані, що можуть створювати підвищений ризик для особи.

3. ЗБІР ЧУТЛИВИХ ДАНИХ

3.1. Збір допускається лише за наявності правових підстав та реальної необхідності.
3.2. Перед збором повинно бути визначено: мету; обсяг; категорію даних; строки зберігання; рівень захисту; коло осіб, які матимуть доступ.
3.3. Забороняється збір надлишкових даних.

4. ЗГОДА

4.1. Якщо обробка потребує згоди, така згода повинна бути: добровільною; поінформованою; конкретною; належно оформленою.
4.2. Для дітей або інших категорій, де це необхідно, згода оформлюється відповідно до вимог законодавства.

5. ДОСТУП ДО ЧУТЛИВИХ ДАНИХ

5.1. Доступ надається виключно окремо визначеним особам.
5.2. Доступ обмежується: роллю; необхідністю; строком; функціями; рівнем ризику.
5.3. Доступ регулярно переглядається.

6. ЗБЕРІГАННЯ

6.1. Чутливі дані зберігаються: лише у визначених середовищах; із підвищеним рівнем захисту; із контролем доступу; із мінімізацією копій; з урахуванням строків зберігання.

7. ПЕРЕДАЧА

7.1. Передача допускається лише за наявності правових або програмних підстав.
7.2. Передача повинна бути: мінімізованою; обґрунтованою; контрольованою; документованою.
7.3. Забороняється: необґрунтована передача; публічне поширення; обговорення у відкритих каналах; передача без належного захисту.

8. ФОТО-, ВІДЕО- ТА МЕДІАМАТЕРІАЛИ

8.1. Використання фото- та відеоматеріалів здійснюється лише: у межах визначеної мети; за наявності правової підстави; із дотриманням вимог згоди; з особливою обережністю щодо дітей та інших вразливих категорій.
8.2. Забороняється використання матеріалів, яке може: створити ризик; завдати шкоди; порушити приватність; принизити гідність особи.

9. АРХІВУВАННЯ ТА ВИДАЛЕННЯ

9.1. Чутливі дані архівуються або видаляються після досягнення мети чи завершення строків.
9.2. Організація забезпечує: контрольоване архівування; посилене зберігання; безпечне видалення; мінімізацію залишкових копій.

10. ІНЦИДЕНТИ

10.1. У разі ризику витоку або компрометації чутливих даних застосовується пріоритетний порядок реагування відповідно до Алгоритму реагування на інциденти.

11. ЗАБОРОНИ

11.1. Забороняється: збір надлишкових даних; передача без підстав; обговорення у відкритих каналах; зберігання у незахищених середовищах; несанкціоноване копіювання; використання всупереч визначеній меті; приховування інцидентів.

12. ВІДПОВІДАЛЬНІСТЬ

12.1. Особи, які працюють із чутливими персональними даними, несуть підвищену персональну відповідальність за: конфіденційність; законність; етичність; безпечність; належне використання.
12.2. Порушення цих Правил може бути підставою для: обмеження доступу; дисциплінарних заходів; припинення співпраці; інших заходів відповідно до внутрішніх процедур Організації.

ДОДАТОК 5

ФОРМА ЗГОДИ НА ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ ГРОМАДСЬКОЇ ОРГАНІЗАЦІЇ «ОСВІТНІЙ КОМПАС»

Я, _____,
дата народження: _____
контактний телефон: _____
електронна пошта: _____
адреса проживання / населений пункт: _____

Підтверджую, що я добровільно, усвідомлено та в межах чинного законодавства України надаю Громадській організації «ОСВІТНІЙ КОМПАС» згоду на обробку моїх персональних даних з метою:
- участі у програмах, проєктах, заходах, навчальних або правозахисних ініціативах;
- комунікації;
- адміністрування участі;
- надання послуг;
- ведення внутрішньої документації;
- моніторингу;
- звітності;
- виконання грантових або партнерських зобов'язань;
- забезпечення безпеки діяльності Організації.

До таких персональних даних належить:
- ПІБ;
- контактні дані;
- дата народження;
- місце проживання;
- соціальний або статусний опис;
- відомості про участь у програмах;
- фото- та відеоматеріали (за потреби);
- документи, надані мною;
- інші дані, необхідні для визначеної мети.

Підтверджую, що ознайомлений(а) з метою збору даних; розумію обсяг даних; поінформований(а) про порядок використання; поінформований(а) про строки зберігання; знаю про право відкликати згоду у випадках, передбачених законодавством; розумію, що Організація застосовує заходи цифрової безпеки для захисту моїх даних.

Окрема згода на фото-/відеофіксацію:
☐ Надаю згоду
☐ Не надаю згоду
на використання фото-, відео- та інших медіаматеріалів із моєю участю в межах: звітності; комунікаційних матеріалів; інформаційних кампаній; програмної діяльності Організації.

Згода діє протягом строку, необхідного для реалізації визначеної мети обробки персональних даних, якщо інше не передбачено законодавством або окремими умовами.

Дата: «___» _____ _____ року
Підпис: _____
ПІБ: _____

ДОДАТОК 6

ФОРМА ОЗНАЙОМЛЕННЯ З ПОЛІТИКОЮ ЦИФРОВОЇ БЕЗПЕКИ ТА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ГРОМАДСЬКОЇ ОРГАНІЗАЦІЇ «ОСВІТНІЙ КОМПАС»

Я, _____,
роль / посада / формат залучення: _____.
контактні дані: _____.

Підтверджую, що:

- ознайомився(лася) з Політикою цифрової безпеки та захисту персональних даних Громадської організації «ОСВІТНІЙ КОМПАС»;
- ознайомився(лася) з додатками до Політики;
- розумію основні принципи, правила та вимоги щодо: захисту персональних даних; конфіденційності; використання цифрових ресурсів; управління доступами; реагування на інциденти; роботи з чутливими категоріями даних;
- зобов'язуюсь дотримуватися положень Політики та внутрішніх процедур Організації.

Підтверджую своє зобов'язання:

- використовувати інформаційні ресурси Організації виключно в межах визначених функцій;
- не передавати доступи третім особам;
- дотримуватись вимог конфіденційності;
- забезпечувати безпечне використання цифрових інструментів;
- повідомляти про інциденти або потенційні ризики;
- дотримуватись правил роботи з персональними та чутливими даними;
- виконувати внутрішні інструкції та процедури.

Підтверджую, що:

- мені зрозумілі основні вимоги;
- я усвідомлюю персональну відповідальність за їх порушення;
- мені відомо про можливість обмеження доступу, дисциплінарних заходів або припинення співпраці у разі недотримання Політики.

Дата ознайомлення: «___» _____ _____ року
Підпис: _____
ПІБ: _____

Відповідальна особа:
ПІБ: _____
Посада / роль: _____
Підпис: _____
Дата: «___» _____ _____ року

ДОДАТОК 7

ЖУРНАЛ ІНЦИДЕНТІВ ЦИФРОВОЇ БЕЗПЕКИ ГРОМАДСЬКОЇ ОРГАНІЗАЦІЇ «ОСВІТНІЙ КОМПАС»

№	Дата та час виявлення	Особа, яка повідомила	Тип інциденту	Короткий опис події	Рівень ризику	Вжиті заходи	Дата закриття	Профілактичні заходи / висновки
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								

ДОДАТОК 8

РЕЄСТР ДОСТУПІВ ДО ІНФОРМАЦІЙНИХ РЕСУРСІВ ГРОМАДСЬКОЇ ОРГАНІЗАЦІЇ «ОСВІТНІЙ КОМПАС»

№	ПІБ особи	Посада / роль	Інформаційний ресурс	Рівень доступу	Дата надання доступу	Дата припинення доступу	Примітки
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							