# РІШЕННЯ КОМІСІЇ

#  від 16 серпня 2006 року C( 2006 ) 3602

**стосовно безпеки інформаційних систем, що використовуються Європейською комісією**

КОМІСІЯ ЄВРОПЕЙСЬКИХ СПІЛЬНОТ,

Беручи до уваги Договір про заснування Європейської Спільноти, зокрема, Статтю 218(2) цього договору,

Беручи до уваги Договір про заснування Європейської спільноти з атомної енергії, зокрема, Статтю 131 цього договору,

Беручи до уваги Договір про Європейський Союз, зокрема Статті 28(1) та 41(1) цього договору,

Оскільки:

1. Інформаційні системи відіграють важливу роль у зборі, введенні, обробці, зберіганні й розповсюдженні інформації.
2. Інформаційні системи можуть бути відкритими для випадкових і навмисних, матеріальних і нематеріальних загроз.
3. Повинна бути система поглядів, що дозволяє визначити загальні принципи, процедури, пріоритети й відповідальності, та основи для вираження потреб в галузі безпеки, для того, щоб кожна інформаційна система могла бути захищеною таким засобом, який відповідає фактичному ступеню ризику, якому вона піддається.
4. Захист інформаційних систем повинен включати заходи щодо технічної та фізичної безпеки, процедурні заходи та організаційні заходи.
5. Умовно горизонтальний характер інформаційних систем означає, що заходи безпеки включають, на різних рівнях, ряд підрозділів, в тому числі горизонтальні підрозділи Комісії.
6. Управління заходами та їх реалізація, спрямовані на забезпечення безпеки інформаційних систем, є відповідальністю кожного Генерального директорату та підрозділу та кожного органу, що використовує інформаційні системи Комісії.
7. Комісія має особливу відповідальність, з одного боку, за захист інформації та інформаційних систем, що належать її Генерального директорату і, з іншого боку, за виконання своїх зобов’язань щодо надання інформації іншим інститутам, державам-членам, громадянам та своїм численним партнерам.
8. Повинні бути єдині правила для того, щоб забезпечити всім інформаційним системам Комісії однаковий захист від загроз, незалежно від Генерального директорату або підрозділу, що володіє ними та незалежно від місця роботи, де вони розташовані.
9. Стосовно системного управління безпекою інформаційних систем, Комісія може застосовувати міжнародно-визнані стандарти, такі як стандарт ISO/IEC 27001. Комісія може також враховувати результати досліджень, які вона безпосередньо здійснює або фінансує відповідно до її рамкових програм наукових досліджень та технологічного розвитку, а також роботу, що проводиться Європейським агентством з мережевої та інформаційної безпеки, встановленого Регламентом (ЄC) № 460/2004 Європейського Парламенту та Ради1.
10. Управління ризиками, пов’язаними з безпекою інформаційних систем є доповненням до управління ризиками, пов’язаними з системами й процедурами внутрішнього контролю Комісії. Воно також доповнює особливий порядок управління ризиками, що складається з оцінки впливу й попередньої оцінки законодавчих пропозицій та основних програм Комісії, які впливають на бюджет 2.
11. Це Рішення застосовується, не обмежуючи Регламенту (ЄС) №1049/2001 Європейського Парламенту та Ради від 30 травня 2001 рокупро доступ громадськості до документів Європейського Парламенту, Ради та Комісії3, Регламенту (ЄС) №45/2001 Європейського Парламенту та Ради від 18 грудня 2000 року про захист фізичних осіб під час обробки персональних даних установами та органами Спільноти та вільного обігу цих даних4, та Директиви 2002/58/ЄC Європейського Парламенту та Ради від 12 липня 2002 року щодо обробки персональних даних та захисту приватності в секторі електронних засобів зв’язку (Директива про захист приватності та комунікації)5.
12. Розділ 25 положень Комісії з безпеки, що є додатком до Рішення 2001/844/ЄC, ЄСВС, Євратом6, містить правила щодо безпеки інформаційних систем, зокрема, ті, які відносяться до секретної інформації ЄС. Ці правила треба розширити, щоб охопити всі інформаційні системи таким чином, щоб захистити цілісність, доступність і конфіденційність цих систем та інформацію, яку вони обробляють.
13. Необхідно оновити Рішення № C(95) 1510 про безпеку інформаційних систем у світлі технологічних розробок та змін в організації Комісії. Задля ясності воно повинно бути замінено на це Рішення,

1 Офіційний вісник Європейського Союзу 77, 13.3.2004, с. 1.

2 SEC (2005) 1327/4 від 25 жовтня 2005 року: “Повідомлення Комісії пані Grybauskaité за погодженням з Президентом і віце-президентом Kallas - На шляху до ефективного й послідовного управління ризиками в службах Комісії ”

3 OJ L 145, 31.5.2001, с. 43.

4 OJ L 8, 12.1.2001, с. 1.

5 OJ L 201, 31.7.2002, с. 37.

6 OJ L 317, 3.12.2001,с. 1.

ПРИЙНЯЛА ТАКІ РІШЕННЯ:

*Стаття 1*

*Предмет*

1. Це Рішення передбачає заходи безпеки для захисту інформаційних систем Комісії та інформації, що обробляється в них, від загроз для її доступності, цілісності й конфіденційності цих систем та інформації.
2. Заходи, що вживаються, можуть бути технічними, фізичними, процедурними або організаційними. Вони повинні сприяти зменшенню ймовірності загроз, щоб зменшити їх вплив, коли вони матеріалізуються, щоб виявити всі випадки порушення безпеки якомога швидше і повернути ситуацію до нормального стану впродовж необхідного терміну.
3. Вони повинні бути у відповідності до ступеню небезпеки з точки зору витрат і функціональних або технічних обмежень.

*Стаття 2 Обсяг*

Заходи безпеки, передбачені цим Рішенням застосовуються до інформаційних систем Комісії та стосуються всіх її Генеральних директоратів та підрозділів у всіх місцях роботи, в тому числі Центру об’єднаних досліджень та делегацій у третіх країнах, офісів, що адміністративно пов’язані з Комісією7 та всіх Виконавчих Агентств або інших органів, що використовують інформаційні системи Комісії. Вони також застосовуються до будь-якої форми дистанційної роботи.

Вони повинні застосовуватися до посадових осіб та інших службовців Спільноти, осіб, що працюють за контрактом Комісії та субпідрядників, які мають доступ й використовують інформаційні системи Комісії.

*Стаття 3 Визначення*

Задля цілей цього Рішення використовуються наступні визначення:

1. “Інформація” означає дані у формі, яка дозволяє передавати їх, записувати або обробляти.
2. “Секретна інформація ЄС” означає всю інформацію, що класифікується як ОБМЕЖЕНО ЄС, КОНФІДЕНЦІЙНО ЄС, ТАЄМНО ЄС або ЦІЛКОМ ТАЄМНО ЄС відповідно до пункту 4.2a положень про безпеку, що є додатком до Рішення 2001/844/ЄC, ЄСВС, Євратом.

7 OLAF, EPSO, OPOCE, OIL, OIB та PMO.

1. “Інформаційна система” означає набір обладнання, методів і процедур, а також у відповідних ситуаціях осіб, персоналу, організованого для здійснення функцій обробки інформації.
2. “Загроза” означає потенціал для випадкового або навмисного порушення безпеки, в тому числі втрату однієї або більше властивостей конфіденційності, цілісності та доступності інформаційних систем або інформації, що в них міститься.
3. “Вразливість” означає слабкість або відсутність запобіжних заходів, які б могли сприяти або дозволити матеріалізацію загрози інформаційній системі або інформації, що в ній міститься.
4. “Ризик” означає ступінь небезпеки того, що загроза може матеріалізуватися, якщо одна або декілька вразливостей в інформаційній системі будуть використаними.
5. “Доступність” означає здатність інформаційної системи виконувати завдання за певних умов відносно графіків, термінів та продуктивності.
6. “Цілісність” означає гарантію того, що інформаційна система та оброблена інформація можуть бути змінені тільки шляхом навмисних і законних дій та що система буде видавати очікуваний результат точно і в повному обсязі.
7. “Конфіденційність” означає замкнутий характер інформації, всієї або частини інформаційної системи (таких як алгоритми, програми та документація), до яких доступ є обмеженим уповноваженими особами, органами та процедурами.
8. “Незаперечення” означає можливість визначення з упевненістю, що дія або подія пов’язані з процесом або особою.
9. “Потреби безпеки” означає точне та однозначне визначення рівнів конфіденційності, цілісності та доступності, пов’язаних зі складовими інформації або інформаційної системи, з метою визначення рівня необхідного захисту.
10. “Вимоги безпеки” означає детальні інструкції відносно функцій або рівнів гарантій, що стосуються заходів безпеки, які буде використано в інформаційній системі, щоб забезпечити їх відповідність потребам безпеки.
11. “Політика забезпечення безпеки інформаційних систем” означає поточні положення, що регулюють інформаційну безпеку, і їх докладні правила реалізації.
12. “План забезпечення безпеки” означає документ, що описує заходи, необхідні для задоволення вимог безпеки інформаційної системи.
13. “Інцидент безпеки” означає подію, яка розцінюється як та, що має шкідливий вплив на безпеку інформаційної системи.
14. “Персональні дані” означає персональні дані, як визначено у Статті 2(a) Регламенту (ЄC) № 45/2001.
15. “Обробка персональних даних” означає обробку персональних даних, як це визначено у Статті 2(b) Регламенту (ЄC) № 45/2001.
16. “Користувач” означає будь-яку особу, до якої застосовується це Рішення.
17. “Генеральний директорат” означає будь-який Генеральний директорат або підрозділи або будь-які інші адміністративні органи, до яких відноситься Стаття 2.
18. “Власник даних” означає будь-якого користувача, котрий як власник інформації забезпечує послідовність та достовірність даних.
19. “Спеціаліст з системної безпеки” (ССБ) означає службовця, призначеного власником інформаційної системи з метою надання рекомендацій власнику щодо безпеки інформаційної системи.

*Стаття 4*

*Дотримання користувачами політики безпеки інформаційних систем*

1. Генеральний директорат повинен вжити необхідних заходів, за допомогою Директорату з питань безпеки, щоб гарантувати, що їх співробітників, в тому числі, субпідрядників та підрядників, було проінформовано про політику безпеки інформаційних систем.
2. Кожен новий користувач повинен бути проінформований про політику безпеки інформаційних систем.
3. Використовуючи ІТ-ресурси Комісії вперше, користувачі вважаються зобов’язаними дотримуватися політики безпеки інформаційних систем.
4. Використання інформаційних систем Комісії з порушенням політики безпеки інформаційних систем або в незаконних цілях може призвести до дисциплінарної відповідальності.
5. Правила щодо використання та доступу з боку користувачів описані в Додатку III.

*Стаття 5*

*Захист персональних даних*

1. Політика безпеки інформаційних систем повинна гарантувати високий рівень захисту персональних даних та їх обробки відповідно до Регламенту (ЄC) № 45/2001, зокрема Статей з 21 до 23 та з 35 до 37.

*Стаття 6*

*Використання технологій шифрування*

1. Використання технологій шифрування Генеральним директоратом повинно бути попередньо схваленим Директоратом з питань безпеки.
2. Генеральний директорат повинен ввести в дію засоби відновлення даних, що зберігаються, там, де необхідний ключ дешифрування не доступний.
3. Там де необхідність належним чином встановлена, відновлення зашифрованих даних здійснюється посадовими особами Директорату з питань безпеки з дозволу його директора або ж здійснюється спеціалістом з безпеки локальної інформації (LISO), згідно з процедурами, які захищають секретну інформацію і персональні дані.

*Стаття 7 Інциденти безпеки*

1. Коли інцидент безпеки, охоплений цим Рішенням, виявляється у Генеральному директораті, спеціаліст з безпеки локальної інформації (LISO) повинен бути проінформований. LISO повинні негайно сповістити про це своїх керівників та Директорат з питань безпеки.
2. Виключно для цілей перевірки й розслідування інцидентів безпеки в інформаційних системах з метою визначення їх причин, наслідків та засобів правового захисту, Директор Директорату з питань безпеки повинен уповноважити посадових осіб директорату отримати доступ до всієї необхідної інформації, де це потрібно, використовуючи належні засоби та відповідно до серйозності випадку, після отримання конкретної згоди Генерального директора Генерального директорату з питань кадрової політики та управління, та після консультацій зі Спеціалістом з захисту даних. Доступ до секретної інформації повинен надаватися відповідно до правил, що регулюють таку інформацію.

*Стаття 8*

*Потреби безпеки інформації та інформаційних систем*

1. Потреби безпеки інформаційних систем та інформації, що в них обробляється, повинні бути виражені стосовно рівня їхньої конфіденційності, цілісності та доступності. Вимоги безпеки визначається на основі цих потреб.
2. Рівні конфіденційності, цілісності та доступності визначені у Додатку I.

*Стаття 9*

*Відповідальності та організація*

1. Відповідальність за безпеку інформаційних систем повинна бути покладена на різні сторони, зокрема, наступні:
	1. Генеральний директорат з питань інформатики, стосовно його керівництва та координації ІТ та телекомунікаційних технологій, що призначені для користування іншими Генеральними директоратами;
	2. Директорат з питань безпеки, стосовно складання та оновлення докладних правил реалізації цього Рішення, стосовно підтримки та моніторингу реалізації політики безпеки інформаційних систем, та стосовно рекомендацій, наданих іншим Генеральним директоратам і підрозділам;
	3. всі Генеральні директорати та підрозділи, стосовно реалізації заходів безпеки для інформаційних систем, за які вони несуть відповідальність.
2. Відповідальності різних сторін за безпеку інформаційних систем та організацію, які повинні бути введеними в дію у Комісії, визначені в Додатку II.

*Стаття 10*

*Докладні правила реалізації*

1. Докладні правила реалізації цього Рішення повинні бути визначені та оновлені Генеральним директором Генерального директорату з питань управління та кадрової політики, який діє на основі пропозицій Директорату з питань безпеки, після консультацій з Генеральним директоратами відповідно до Статті 23 Процесуальних норм Комісії, та після інформування Європейського інспектора із захисту даних відповідно до Статті 28(1) Регламенту (ЄC) № 45/2001.
2. Розробка і коригування докладних правил реалізації повинні враховувати наступне:
	1. нові зобов’язання, якими може бути зв’язана Комісія,
	2. розробки в галузі ІТ та технологій електронної комунікації, зокрема результати дослідницької роботи, яка проводиться та фінансується Комісією,
	3. досвід, накопичений в галузі застосування політики безпеки інформаційних систем,
	4. конкретні ситуації у Генеральних директоратах та підрозділах, таких як Європейська служба боротьби проти шахрайства, делегаціях, представництвах та іноземних офісах,
	5. міжнародно-визнані норми і стандарти, що діють в області безпеки інформаційних систем,
	6. робота, що проводиться Європейським агентством з мережевої та інформаційної безпеки.
3. Докладні правила можуть бути доповнені заходами технічного, фізичного, процесуального або організаційного характеру, затвердженими Генеральним директором Генерального директорату з питань управління та кадрової політики за погодженням з підрозділами, що мають законний інтерес.

*Стаття 11 Перехідні положення*

1. Будь-яка нова інформаційна система повинна ще на стадії проектування враховувати політику безпеки інформаційних систем.
2. Політика безпеки інформаційних систем повинна бути введена до діючих інформаційних систем в межах строку, узгодженого спільно відповідним Генеральним директоратом та Директоратом з питань безпеки.

*Стаття 12 Припинення дії*

Рішення C (95) 1510 від 23 листопада 1995 року, таким чином, скасовується.

Підписано в Брюсселі, 16 серпня 2006 року

*Для Комісії*

*Член Комісії*

# ДОДАТОК I

**Конфіденційність, цілісність та доступність**

* 1. **ВИЗНАЧЕННЯ РІВНЯ КОНФІДЕНЦІЙНОСТІ ІНФОРМАЦІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ**
		1. Без шкоди для класифікацій, передбачених положеннями про безпеку, інформаційні системи та інформація, що в них обробляється, повинні бути захищені з метою забезпечення того, що тільки уповноважені особи або ті, яким необхідно знати, можуть отримати до них доступ або ж отримати з них інформацію.
		2. З метою забезпечення відповідних заходів безпеки, інформаційні системи та інформація, що в них обробляється, повинні бути визначені відповідно до їхнього рівня конфіденційності, залежно від ймовірних наслідків, які несанкціоноване відкриття може мати для інтересів Комісії, інших установ, держав-членів або інших сторін.
		3. Рівні, зазначені в пункті 2, наступні:
			+ “ЗАГАЛЬНИЙ”: інформаційна система або інформація, публічне розкриття якої не завдасть шкоди інтересам Комісії, інших установ, держав-членів або інших сторін;
			+ “ОБМЕЖЕНИЙ”: інформаційна система або інформація, що призначається для обмеженої кількості осіб за принципом службової необхідності, розкриття якої не уповноваженим особам може заподіяти шкоди Комісії, іншим установам, державам-членам або іншим сторонам, але не настільки серйозної шкоди, щоб відносити це до класифікації, зазначеної в пункті 16.1 положень про безпеку. Додаткове маркування повинне бути доданим для інформації на цьому рівні безпеки з визначенням категорій осіб або органів, які є одержувачами інформації або уповноважені мати доступ до неї.
	2. **ВИЗНАЧЕННЯ РІВНІВ ЦІЛІСНОСТІ ТА ДОСТУПНОСТІ ІНФОРМАЦІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ**
		1. Інформаційні системи та інформація, що в них обробляється, також повинні бути визначені відповідно до рівня їхньої цілісності та доступності залежно від ймовірних наслідків, які втрата цілісності або доступності може мати для інтересів Комісії, інших установ, держав-членів або інших сторін.
		2. Рівні, зазначені в пункті 1, наступні:
			+ “СЕРЕДНІЙ” застосовується до інформації або інформаційних систем, втрата цілісності або доступності яких може загрожувати внутрішній роботі Комісії; ці випадки будуть включати незастосування процесуальних норм без будь-якого зовнішнього впливу або з обмеженим зовнішнім впливом, загрозу для досягнення цілей плану дій, або виникнення суттєвих організаційних та робочих проблем в межах Комісії без будь-якого зовнішнього впливу;
			+ “КРИТИЧНИЙ” застосовується до інформації або інформаційних систем, втрата цілісності або доступності яких може загрожувати позиції Комісії щодо інших установ, держав-членів або інших сторін; ці випадки будуть включати шкоду іміджу Комісії або інших установ в очах держав-членів або громадськості, дуже серйозну шкоду, завдану юридичним або фізичним особам, перевитрати бюджету або значні фінансові втрати з дуже серйозними негативними наслідками для фінансової системи Комісії;
			+ “СТРАТЕГІЧНИЙ” застосовується до інформації або інформаційних систем, втрата цілісності або доступності яких буде неприйнятною для Комісії, інших установ, держав-членів або інших сторін, тому що це може, наприклад, призвести до призупинення процесу прийняття рішень Комісією, негативно вплинути на важливі переговори, що спричинить катастрофічні політичні збитки та фінансові втрати, або зірве виконання умов Договорів або їх застосування.
	3. **ВИМОГИ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ**
		1. Вимоги безпеки інформаційних систем визначаються на основі їхніх потреб у галузі безпеки та потреб безпеки інформації, яку вони обробляють. Правила та рекомендації, що регулюють таке визначення, повинні бути встановлені в докладних правилах реалізації.
		2. В цілях проведення інвентаризації та звітності, інформаційні системи повинні бути класифіковані з точки зору вимог до їх безпеки, як визначено у попередньому пункті, наступним чином:
			+ “СТАНДАРТНІ”: де вимоги безпеки відповідають заходам безпеки, передбаченим основною інфраструктурою інформаційних систем Комісії, чия інфраструктура повинна бути визначена у докладних правилах реалізації;
			+ “СПЕЦИФІЧНІ”: де вимоги безпеки спричиняють необхідність ввести в дію заходи, які доповнюють або замінюють заходи безпеки, передбачені інфраструктурою інформаційних систем Комісії.
		3. Акредитація інформаційних систем, що обробляють секретну інформацію, повинна регулюватися Розділом 25 положень про безпеку, що є додатком до Рішення № 2001/844/ЄC, ЄСВС, Євратом.

# ДОДАТОК II

**Відповідальності різних сторін за безпеку інформаційних систем**

1. **ГЕНЕРАЛЬНИЙ ДИРЕКТОРАТ**
	1. Генеральні директорати несуть відповідальність за реалізацію політики безпеки інформаційних систем для інформаційних систем, що знаходяться в межах їх відповідальності. Вони несуть відповідальність за діяльність, пов’язану з управлінням цією реалізацією.
	2. Генеральні директорати складають, впроваджують та керують планами забезпечення безпеки для своїх інформаційних систем. Ці плани повинні бути внесені в реєстр.
	3. Вони повинні визначити і спланувати основні напрямки, людські ресурси, бюджетні ресурси та ІТ-ресурси для діяльності, пов’язаної з їх відповідальністю за безпеку інформаційних систем.
	4. Генеральні директорати можуть делегувати всю або частину реалізації та управління їхніми планами забезпечення безпеки у горизонтальні підрозділи, такі як Генеральний директорат з питань інформатики. У таких випадках Генеральні директорати повинні гарантувати, що підрозділ, про який йдеться, вживає необхідні заходи безпеки. Задля визначення умов делегування, між сторонами треба укласти Угоду про рівень обслуговування, яка визначає, зокрема, заходи з моніторингу реалізації.
	5. Генеральні директорати повинні своєчасно сповіщати Генеральний директорат з питань інформатики, спеціалістів з безпеки локальної інформації, спеціалістів з безпеки локальної інформації інших Генеральних директоратів та Директорату з питань безпеки про будь-які зміни в архітектурі їхніх систем, які ймовірно можуть вплинути на інформаційні системи, які не знаходяться в межах їхньої відповідальності.
	6. Вони повинні періодично проводити аналіз вимог безпеки своїх інформаційних систем, виходячи з потреб у галузі безпеки.
	7. Вони повинні скласти, реалізувати та розробити відповідні заходи для своїх інформаційних систем відповідно до вимог щодо їх безпеки для того, щоб надати їм належний захист.
	8. Вони повинні створювати, підтримувати та перевіряти плани дій у непередбачених обставинах та плани резервного копіювання з урахуванням потреб у галузі безпеки.
	9. Вони повинні гарантувати, що зобов’язання дотримуватися політики безпеки інформаційних систем Комісії чітко визначені у кожному контракті, який вони укладають з підрядниками.
2. **СПЕЦІАЛІСТИ З БЕЗПЕКИ ЛОКАЛЬНОЇ ІНФОРМАЦІЇ (LISO)**
	1. Кожен Генеральний директор або начальник служби призначає принаймні одного спеціаліста з безпеки локальної інформації (LISO). LISO не повинні бути членами команди управління інформаційною безпекою та повинні звітувати безпосередньо перед Генеральним директором, начальником служби або начальником управління ресурсами. Не повинно бути ніякого ієрархічного зв’язку між LISOs та Директоратом з питань безпеки.
	2. LISO повинні бути достатньо доступними, мати відповідний досвід в галузі безпеки інформаційних систем та мати навички управління, необхідні для ефективного виконання їх ролі.
	3. В межах свого Генерального директората, LISO
		* повинні здійснювати контроль за розробкою планів забезпечення безпеки, затверджених Генеральним директором та контролювати їх реалізацію,
		* повинні сприяти поширенню політики безпеки інформаційних систем в рамках Генерального директорату, пропонуючи конкретні інформаційно-освітні та навчальні програми,
		* повинні забезпечити, щоб інвентаризація всіх інформаційних систем підтримувалась та оновлювалась, з описом потреб в галузі безпеки та класифікації вимог,
		* повинні давати поради та доповідати їхньому керівництву, власникам системи, постачальникам ІТ-послуг та керівникам проектів стосовно питань в галузі безпеки інформаційних систем,
		* повинні забезпечити, щоб постачальники ІТ-послуг та системні постачальники ввели в дію в інформаційних інфраструктурах або системах заходи безпеки, необхідні у відповідності з планами забезпечення безпеки.
		* повинні співпрацювати з спеціалістом з локальної безпеки (LSO), визначеним у положеннях з питань безпеки, що є додатком до Рішення № 2001/844/ЄC, ЄСВС, Євратом,
		* повинні співпрацювати з Координатором з захисту даних (DPC), визначеним у SEC (2002) 1043,
		* повинні бути головними контактними особами Директорату з питань безпеки стосовно безпеки інформаційних систем та брати участь у цій якості у зустрічах, організованих ним.
	4. Без шкоди для положень з питань безпеки, прикріплених до Рішення № 2001/844/ ЄC, ЄСВС, Євратом, LISO можуть приймати участь у перевірках, що проводяться кожного разу, коли відбувається інцидент безпеки, який може загрожувати одній або декільком інформаційним системам, що використовуються їхнім Генеральним директоратом, з метою встановлення його причин та впливу та визначення стримуючих та коригувальних заходів.
3. **ВЛАСНИКИ СИСТЕМИ**
	1. Власники системи повинні нести відповідальність за безпеку своєї інформаційної системи. Вони повинні визначати потреби в галузі безпеки інформаційної системи та інформації, яка в ній обробляється. З цією метою вони повинні взяти до відома потреби, виражені власниками даних та користувачами.
	2. У питаннях безпеки інформаційних систем, вони повинні радитися з спеціалістом з безпеки локальної інформації їхнього Генерального директорату або зі спеціалістом з системної безпеки (SSO), яких вони, можливо, призначили для цієї мети.
	3. Вони мають затвердити визначення вимог безпеки та заходів безпеки.
	4. Вони повинні зробити запит на акредитацію у Органа з акредитації безпеки (SAA) для будь-якої інформаційної системи, яка потребує акредитації з метою застосування положень про безпеку8. Вони повинні гарантувати, що їхня інформаційна система відповідає рішенням Органа з акредитації безпеки.
	5. **ВЛАСНИКИ ДАНИХ**

**5.** Власники даних повинні забезпечувати послідовність і достовірність інформації в локальному домені, в якому використовується інформаційна система. Вони повинні визначити потреби безпеки даних, за які вони несуть відповідальність та проінформувати власників системи про ці потреби.

* 1. **СПЕЦІАЛІСТИ З СИСТЕМНОЇ БЕЗПЕКИ (SSO)**
1. Вони повинні забезпечити, щоб безпека системи відповідала принципам цього Рішення та здійснювати необхідну політику з безпеки в цьому відношенні.
2. Вони повинні координувати свою діяльність з діяльністю LISO.
3. Вони повинні ретельно розробити визначення, реалізацію та перевірку потреб безпеки системи, за які вони несуть відповідальність.
4. Вони повинні повідомляти власнику інформаційної системи все, що стосується питань безпеки.
5. **КЕРІВНИКИ ПРОЕКТІВ**
	1. Керівники проектів повинні нести відповідальність за встановлення та передачу інформаційної системи власнику системи. Вони повинні вказати вимоги безпеки на основі потреб безпеки, визначених останніми, в світлі оцінки ризиків у разі потреби. Вони повинні визначити архітектуру, застосувати звичайні заходи з безпеки Комісії та визначити й реалізувати конкретні заходи щодо забезпечення безпеки. Вони повинні забезпечити, щоб ці заходи були введені в дію в інформаційній системі або в інфраструктурах, які її підтримують, чи то локальних або централізованих.
	2. Вони повинні співпрацювати з організаціями INFOSEC, Crypto та TEMPEST, визначеними у положеннях з безпеки, що є додатком до Рішення 2001/844/ЄC, ЄСВС, Євратом під час розробки документів, необхідних для процедури акредитації та відповідності системи рішенням Органа з акредитації безпеки.

8 Акредитація визначена у пункті 25.2 положень про безпеку, що є додатком до Рішення 2001/844/ЄC, ЄСВС, Євратом.

1. Вони повинні гарантувати, що розробка, реалізація та виконання проекту відповідають вимогам безпеки інформаційної системи та політики безпеки інформаційних систем.
2. **СИСТЕМНІ ПОСТАЧАЛЬНИКИ**
	1. Системні постачальники повинні створювати та забезпечувати підтримку та розвиток інформаційної системи відповідно до вимог безпеки, укладених керівником проекту та затверджених власником системи.
	2. Вони повинні визначити технічну архітектуру спільно з Генеральним директоратом з питань інформатики, та укласти технічні специфікації для реалізації вимог безпеки, як визначено керівником проекту.
	3. Вони повинні забезпечити посібниками з експлуатації та інструкціями.
3. **СИСТЕМНИЙ МЕНЕДЖЕР**
	1. Системні менеджери повинні керувати роботою інформаційної системи від імені власника системи. Вони можуть керувати конкретними заходами з безпеки безпосередньо, або передовірити їхнє керування постачальникам ІТ-послуг. В останньому випадку, вони повинні укласти Угоду про рівень обслуговування з постачальниками ІТ-послуг для того, щоб упевнитися в тому, що заходи безпеки, за які вони відповідають, реалізуються.
	2. Вони повинні гарантувати, що інформація, необхідна для задоволення потреби незаперечення та моніторингу належного виконання Угоди про рівень обслуговування, зберігається і є доступною.
4. **ПОСТАЧАЛЬНИКИ IT-ПОСЛУГ**
	1. Постачальники ІТ-послуг повинні надати власникам системи низку структурованих та керованих ІТ-ресурсів, таких як мережі електронних комунікацій, обладнання та програмне забезпечення.
	2. Функції постачальників ІТ-послуг повинні здійснюватися, зокрема, підрозділами Генерального директорату з питань інформатики, деякими підрозділами Комісії, менеджерами інформаційних ресурсів (IRM) або субпідрядними зовнішніми послугами.
	3. Постачальники ІТ-послуг повинні нести відповідальність за управління безпекою ресурсів, які вони надають.
	4. Вони повинні здійснювати заходи безпеки, зазначені в Угодах про рівень обслуговування, укладених з системними менеджерами, у планах з безпеки та домовленостях, досягнутих з іншими постачальниками послуг.
	5. Вони повинні вести вичерпний перелік ІТ-ресурсів, якими вони керують. Для кожного такого ресурсу інвентаризація має встановлювати вимоги безпеки, яким вони повинні відповідати.
	6. Вони повинні інформувати відповідних системних менеджерів та LISO про будь-які інциденти безпеки, які відбуваються.
	7. Вони повинні здійснювати запобіжні та коригувальні заходи безпеки, коли стається інцидент безпеки, спільно з Директоратом з питань безпеки та LISO.
	8. Вони повинні підтримувати рівень безпеки своїх ІТ-ресурсів, застосовуючи політику безпеки інформаційних систем.
	9. Вони повинні оцінювати вплив на безпеку змін, внесених до ІТ-ресурсів. Повинні інформувати відповідних LISO про зміни у рівні безпеки. Вони також повинні інформувати Європейську ІТ-спільноту та Директорат з питань безпеки, якщо зміни, ймовірно, будуть мати вплив на інформаційні системи Комісії, які знаходяться поза зоною їхнього контролю.
	10. Вони повинні гарантувати, що нове програмне забезпечення або обладнання, яке буде встановлене, є безпечним для інформаційних систем та інформації, що в ній обробляється.
	11. Вони повинні контролювати доступність ІТ-ресурсів.
	12. Вони повинні ввести в дію плани дій у непередбачуваних обставинах та плани резервного копіювання для ІТ-ресурсів, якими вони керують.
	13. Вони мають впровадити, або спричинити впровадження заходів забезпечення фізичної безпеки для захисту обладнання, за яке вони несуть відповідальність, вибір заходу має ґрунтуватися на вимогах безпеки, яким повинно відповідати обладнання.
	14. Вони повинні гарантувати, що інформація, необхідна для задоволення потреби не заперечення, зберігається і є доступною.
	15. Вони можуть призначити менеджера з безпеки, завданням якого буде координувати діяльність, пов’язану з оперативним управлянням безпеки послуг, що надаються.
5. **МЕНЕДЖЕРИ ЛОКАЛЬНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ (IRM)**
	1. Менеджери локальних інформаційних ресурсів (IRM) повинні нести відповідальність за забезпечення ІТ-ресурсів у своєму Генеральному директораті. Вони можуть також здійснювати деякі з функцій безпеки, зазначених у цьому Додатку, в залежності від Генерального директората, про який йдеться. Загалом, вони повинні бути постачальником ІТ-послуг для Генерального директорату стосовно локальних ресурсів та їх персонал повинен управляти безпекою цих ресурсів відповідно.
6. **ДИРЕКТОРАТ З ПИТАНЬ БЕЗПЕКИ**
	1. Директорат з питань безпеки повинен нести відповідальність за координацію всіх заходів, пов’язаних з виконанням цього Рішення. Він повинен гарантувати, що заходи послідовні та, що це Рішення виконується відповідно до положень про безпеку.
	2. Він повинен скласти спільно з LISO докладні правила реалізації для цього Рішення, які будуть прийняті відповідно до процедури, зазначеної в Статті 10.
	3. Згідно з положеннями про безпеку, він повинен виступати в ролі Органу з акредитації безпеки (SAA), органу INFOSEC (IA), органу Crypto (CrA) та органу TEMPEST (TA).
	4. Він повинен організувати навчання, інформаційно-роз’яснювальну та допоміжну діяльність спільно з підрозділами, що відповідають за загальне та ІТ-навчання в Комісії з метою забезпечення виконання й застосування цього Рішення.
	5. Він повинен забезпечити, щоб політика безпеки інформаційних систем була врахована, коли Генеральний директорат з питань інформатики та інші Генеральні директорати складають ІТ-стратегію.
	6. Він повинен консультувати і надавати допомогу Генеральним директоратам у впровадженні політики безпеки інформаційних систем і під час складання, виконання і моніторингу планів забезпечення безпеки.
	7. Він має гарантувати, що плани забезпечення безпеки відповідають політиці безпеки інформаційних систем.
	8. Він повинен консультувати і надавати допомогу системним власникам та керівникам проектів під час підготовки документів, необхідних для акредитації та в процесі приведення інформаційних систем у відповідність з рішеннями, прийнятими Органом з акредитації в галузі безпеки.
	9. Він повинен підтримувати тісну співпрацю з LISO. Він повинен консультувати їх та надавати допомогу при виконанні їхніх завдань. Він повинен організувати зустріч з ними, принаймні один раз на рік.
	10. Він повинен підтримувати співпрацю з органами національної безпеки країн-членів і з органами безпеки інших європейських установ, пов’язаних із реалізацією цього Рішення.
	11. Щодо запрошень на участь у тендері, Директорат з питань безпеки може приймати участь, або з власної ініціативи або на прохання Генерального директорату, у складанні технічних специфікацій та критеріїв вибору й присудження по відношенню до безпеки інформаційних систем.
	12. Він повинен здійснювати контроль за виконанням політики безпеки інформаційних систем. Він повинен доповідати з цього питання компетентним органам в Комісії. У разі серйозних порушень, він повинен довести до відома цих органів це питання якомога швидше та, в разі необхідності, довести до відома члена Комісії, який відповідає за питання безпеки.
	13. Потрібен буде його дозвіл на підключення мереж електронних комунікацій до приватної мережі електронних комунікацій Комісії.
7. **ГЕНЕРАЛЬНИЙ ДИРЕКТОРАТ З ПИТАНЬ ІНФОРМАТИКИ**
	1. Правила та обов’язки, встановлені для Генерального директората застосовуються з відповідними змінами до Генерального директората з питань інформатики.
	2. Генеральний директорат з питань інформатики має розробити і підтримувати ІТ-інфраструктуру, в тому числі методологію та виділені ресурси для розвитку інформаційних систем, відповідно до політики безпеки інформаційних систем.
	3. Він повинен гарантувати безпеку приватної мережі електронних комунікацій Комісії та забезпечити безпечні підключення до мережі для зовнішніх сайтів Комісії, підрядників та всіх уповноважених партнерів, спільно з відповідним Генеральним директоратом.
	4. Він має зробити доступну архітектуру, еталонні конфігурації та ІТ-програмне забезпечення та відповідність обладнання потребам реалізації політики безпеки.
	5. Він має розробити і здійснити в рамках Комісії програму заходів щодо запобігання експлуатації вразливостей в системах, таких як заходи по боротьбі зі зловмисним кодом. Він повинен ввести коригувальні заходи для запобігання експлуатації вразливостей в програмному забезпеченні та обладнанні, для якого він забезпечує централізовану підтримку.
	6. Він повинен здійснювати керівництво механізмами загальної безпеки, такими як брандмауери, програми виявлення вторгнень, антивірусні програми та системи аутентифікації.
	7. Він має керувати інцидентами безпеки у співпраці з Управлінням з питань безпеки.
	8. Спільно з Управлінням з питань безпеки Генеральний директорат повинен бути в курсі останніх технологічних розробок щодо безпеки для всього ІТ-програмного забезпечення та обладнання, для якого він забезпечує централізовану підтримку.
	9. Він може делегувати певні завдання та обов’язки в інші підрозділи. У таких випадках має бути укладена Угода про рівень обслуговування між Генеральним директоратом з питань інформатики, відповідним Генеральним директоратом та Директоратом з питань безпеки з метою визначення умов делегування, зокрема, стосовно підключення мереж електронних комунікацій.

# ДОДАТОК III

**Правила використання та доступу до інформаційних систем Комісії**

* + 1. **ЗАГАЛЬНІ ПРАВИЛА**
			1. Користувачі повинні дотримуватись політики безпеки інформаційних систем і планів забезпечення безпеки, що застосовуються до них при виконанні своїх обов’язків.
			2. Без шкоди для інших зобов’язань, що виникають з положень, які можуть застосовуватися до них, користувачі повинні прагнути до того, щоб інформаційні та ІТ-ресурси, надані в їх розпорядження Комісією, були захищені.
			3. Ці правила застосовуються також до дистанційної роботи.
		2. **СПЕЦИФІЧНІ ПРАВИЛА**
			1. Без шкоди для положень Статті 17 Штатного регламенту або інших положень, які можуть застосовуватися, користувачі повинні прагнути забезпечити, щоб інформація, яка є власністю Комісії, не розголошувалась стороннім особам.
			2. Вони повинні використовувати всі засоби для контролю доступу, якими вони забезпечені, з метою запобігання використанню сторонніми особами ресурсів, які знаходяться у їх розпорядженні або під їх контролем. Крім того, вони повинні слідкувати за тим, щоб інформаційні системи, які знаходяться у їх розпорядженні, були недоступними під час їхньої відсутності, навіть тоді, коли це на короткий час.
			3. За виключенням інформаційних систем колективного доступу, вони повинні мати доступ тільки до тих інформаційних систем, для яких їм було надано чіткий дозвіл, незалежно від того, чи є ці системи власністю Комісії.
			4. Вони не повинні розкривати механізми своєї аутентифікації або ділитися ними з іншими людьми.
			5. Вони повинні використовувати інформаційні системи, які знаходяться у їх розпорядженні або під їх контролем так, як вони призначені для використання.
			6. Вони не повинні встановлювати обладнання або програмне забезпечення на ІТ-ресурси, які знаходяться у їх розпорядженні або під їх контролем.
			7. Вони не повинні встановлювати обладнання або програмне забезпечення, які дозволяють підключення до інших мереж електронних комунікацій.
			8. Вони не повинні ані встановлювати, ані використовувати власне обладнання або програмне забезпечення для доступу до інформаційних систем, передбачених цим Рішенням.
			9. Якщо користувачі дізнаються про вразливість або подію, що впливає на одну або декілька інформаційних систем Комісії, вони повинні негайно повідомити про це менеджера локальних інформаційних ресурсів (IRM) свого Генерального директорату або особу, призначену останнім для цієї функції.
			10. Вони не повинні прагнути перевірити будь-які вразливості в системах і не повинні прагнути обійти заходи безпеки, введені в дію.
			11. Вони повинні слідкувати за тим, щоб відвідувачі, за яких вони відповідають, своєю поведінкою не ставили під загрозу безпеку інформаційних систем Комісії, та, зокрема, слідкувати за тим, щоб вони не підключали своє власне обладнання до приватної мережі електронного зв’язку Комісії.
			12. Будь-який відступ від цих правил повинен бути виправданий потребами служби та бути чітко дозволеним LISO та відповідним постачальником ІТ-послуг після інформування Директорату з питань безпеки, який залишає за собою право встановлювати рамки для такого відступу.