ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ "ТЕСТМЕТРСТАНДАРТ"
10003, м. Житомир, майдан Перемоги, будинок 10; тел. (0412) 43-30-20, (067) 464-78-86

ЗВІТ № 2
ПРО АУДИТ СИСТЕМИ МЕНЕДЖМЕНТУ

на відповідність вимогам:

☐ **ДСТУ EN ISO 9001:2018**	☐ **ДСТУ ISO 22000:2019**
☐ **ДСТУ ISO 9001:2015**	☐ **ISO 22000:2018**
☐ **ISO 9001:2015**	☐ **ДСТУ ISO 45001:2019**
☐ **ДСТУ ISO 14001:2015**	☐ **ISO 45001:2018**
☐ **ISO 14001:2015**	☒ **ДСТУ ISO/IEC 27001:2023**

Вид робіт:

☒ Первинна сертифікація

☐ Повторна сертифікація ☐ Розширення сфери сертифікації

Інформація щодо аудиту:

за одним стандартом ☐ скомбінований ☐

інтегрований ☒ спільний ☐

Дати проведення оцінки на місці Початок 11.10.2023 Закінчення 11.10.2023

Місце проведення аудиту: м. Київ, Голосіївський р-н, вул. Антоновича, буд. 23-В

Загальні відомості про організацію-заявника:

Назва	ТОВ «ВІЕНЕРДЖІ»
Юридична адреса	02121, м. Київ, вул. Вербицького Архітектора, буд. 26, кв. 64
Адреса провадження діяльності	01024, м. Київ, Голосіївський р-н, вул. Антоновича, буд. 23-В
Телефон/факс/ e-mail	-

Кількість працівників, що працюють на ділянках, охоплених системою менеджменту:	10
Для систему управління охороною здоров'я та безпекою праці (СУОЗіБП):	
- кількість працівників, що працюють на ділянках, охоплених СУОЗіБП	-
- кількість працівників, що працюють всередині приміщень організації	-
- кількість працівників, що працюють поза межами приміщень організації	-
Наявність філій Так ☐ Ні ☒	
Сезонність виробництва Так ☐ Ні ☒	
Для СКБХП:	
- кількість виробничих ліній	-
- кількість досліджень НАССР	-

Назва продукції/послуг, щодо якої передбачено перевірити (оцінити) систему менеджменту

Неспеціалізована оптова торгівля; оптова торгівля побутовими електротоварами й електронною апаратурою побутового призначення для приймання, записування, відтворювання звуку й зображення, електронним і телекомунікаційним устаткованням, деталями до нього, іншими машинами й устаткуванням; роздрібна торгівля в спеціалізованих магазинах електронною апаратурою побутового призначення для приймання, записування, відтворювання звуку й зображення; інші види роздрібної торгівлі в неспеціалізованих магазинах та поза магазинами, роздрібна торгівля, що здійснюється фірмами поштового замовлення або через мережу інтернет; ремонт і технічне обслуговування електронного й оптичного устаткування та елек-

тричного устаткування; ремонт електронної апаратури побутового призначення для приймання, записування, відтворювання звуку й зображення; діяльність у сфері інжинірингу, геології та геодезії, надання послуг технічного консультування в цих сферах

Порядковий номер виду економічної діяльності

☐	1	☐	15	☒	19	☐	30	☐	36
☐	3	☐	16	☐	23	☐	31	☐	37
☐	12	☐	17	☐	28	☒	34	☐	38
☐	14	☐	18	☒	29	☐	35		

Категорія та підкатегорія харчового ланцюга:

☐	A	☐	C	☐	D	☐	F	☐	H
☐	AI	☐	CI	☐	DI	☐	FI	☐	I
☐	AII	☐	CII	☐	DII	☐	FII	☐	K
☐	B	☐	CIII	☐	E	☐	G		
☐	BI	☐	CIV			☐	GI		
☐	BII					☐	GII		

Виробництво продукції/надання послуг здійснюється згідно з вимогами нормативної документації	Чинного законодавства

2. Підстави для проведення сертифікації

- Заявка № 301 від 29.09.2023 р.;
- Протокол аналізування заявки, затверджений 29.09.2023 р..;
- Програма проведення сертифікації системи менеджменту від 02.10.2023 р.
- План проведення першого етапу аудиту системи менеджменту від 02.10.2023 р.
- Висновок за результатами першого етапу аудиту системи менеджменту від 05.10.2023р.
- План проведення аудиту на місці (другого етапу) системи менеджменту від 10.10.2023р.

3.Цілі, завдання сертифікації

3.1 Ціллю сертифікації є засвідчення відповідності системи менеджменту підприємства вимогам ДСТУ ISO/IEC 27001:2023 і забезпечення впевненості в тому, що підприємство здатне постійно випускати продукцію, яка відповідає вимогам діючих нормативних документів, продукція/послуга незадовільної якості завчасно виявляється та вживаються заходи щодо запобігання випуску такої продукції/надання такої послуги.

3.2 Завдання перевірки – одержання об'єктивних даних щодо:

- відповідності документів системи менеджменту вимогам ДСТУ ISO/IEC 27001:2023;
- впровадження документів системи менеджменту, дотримання їх вимог на ТОВ «ВІЕНЕРДЖІ», розуміння цих вимог його персоналом;
- забезпечення підприємством випуску продукції/надання послуги відповідно до вимог замовників та регламентувальних вимог;
- результативності системи менеджменту стосовно досягнення цілей, що визначені політикою підприємства.

4 Сфера сертифікації

4.1 Підрозділи, в яких проводилася перевірка: все підприємство.

5. Склад комісії з сертифікації системи менеджменту:

	П.І.
Керівник групи аудиту	Оксана Сак
Аудитор	Юлія Герасимчук
Тех. експерти	Віктор Герасимчук

6.Відомості про виконання перевірки:

6.1 Відхилення від плану аудиту ☐ Так ☒ Ні

Якщо «Так» - вказати причини:

6.2 Наявність будь-які значні питання, що впливають на програму аудиту.

☐ Так ☒ Ні

Якщо «Так» - вказати які:

6.3 Невирішені питання:

☐ Так ☒ Ні

Якщо «Так» - вказати які:

7. Методи проведення перевірки:

- опитування;
- вивчення документів;
- обстеження об'єктів виробництва продукції (надання послуг);
- здійснення спостережень на ділянках, що перевіряються;
- оцінка відповідності фактичного стану вимогам нормативних документів та документації системи менеджменту.

8. Загальна характеристика системи менеджменту та характеристика фактичного стану об'єктів перевірки:
Загальна оцінка відповідності системи менеджменту ТОВ «ВІЕНЕРДЖІ» на відповідність вимогам ДСТУ ISO/IEC 27001:2023 подана у таблиці, яка наведена нижче:

ДСТУ ISO/IEC 27001:2023	Назва процедур технічного нагляду	Зауваження, порушення		Зміст зауважень, номер додатку
		так	ні	
1	2	3	4	5
4	Контекст діяльності організації			
	Чи проводиться організацією оцінка результативності дій щодо провадження та функціювання системи управління інформаційною безпекою			
	Чи дії, вжиті організацією в інформаційній безпекищо має встановлювати зобов'язання організації щодо досягнення поліпшення 4.1 Розуміння внутрішніх та зовнішніх факторів діяльності організації В організації визначені зовнішні та внутрішні фактори, що мають відношення до діяльності організації та впливають на її здатність досягати очікуваного(их) результату(ів) від системи менеджменту інформаційної безпеки. 4.2 Розуміння потреб та очікувань зацікавлених сторін Організація має визначити: a) зацікавлені сторони, які стосуються системи менеджменту інформаційної безпеки; b) вимоги цих заінтересованих сторін щодо інформаційної безпеки. Примітка — Вимоги заінтересованих сторін можуть включати правові та нормативні вимоги та договірні зобов'язання. 4.3 Визначення сфери дії системи менеджменту інформаційної безпеки Для встановлення сфери дії системи менеджменту інформаційної безпеки організація повинна визначити застосовність системи менеджменту інформаційної безпеки та її кордону. При визначенні сфери дії системи менеджменту інформаційної безпеки необхідно враховувати: a)внутрішні та зовнішні фактори, зазначені в 4.1; b)вимоги, наведені у 4.2; c)порядок взаємодії та залежності між діяльністю цієї організації та діяльністю		+	

	інших організацій. Область дії системи управління інформаційної безпеки має бути доступна у вигляді документованої інформації. 4.4 Система менеджменту інформаційної безпеки Створення, впровадження, підтримку та постійне покращення системи менеджменту інформаційної безпеки організація повинна проводити відповідно до вимог стандарту.			
5	Керівництво			
	5.1 Вище керівництво повинно продемонструвати дії з управління та зобов'язання по відношенню до систем управління інформаційною безпекою. a) гарантуванням, що політика інформаційної безпеки та цілі інформаційної безпеки розроблені та сумісні зі стратегічними планами організації; b) гарантуванням інтеграції вимог системи інформаційної безпеки в процеси організації; c) гарантуванням, що ресурси, потрібні для системи управління інформаційною безпекою, доступні; d) доведенням до відома організації важливості ефективного управління інформаційною безпекою та відповідності вимогам системи управління інформаційною безпекою; e) гарантуванням, що система управління інформаційною безпекою досягне своїх запланованих результатів; f) призначенням та підтримкою осіб для досягнення ефективності системи управління інформаційною безпекою;g) сприянням постійному вдосконаленню; h) підтримкою інших пов'язаних ролей вищого керівництва, щоб продемонструвати їх керівну роль, яку вони застосовують у сферах їх відповідальності. 5.2 Політика Вище керівництво повинно запровадити політику інформаційної безпеки, яка: a) відповідає цілям організації; b) містить цілі інф ормаційної безпеки або зазначає основні положення для визначення цілей інформаційної безпеки; c) містить зобов'язання відповідати застосованим вимогам, пов'язаним з інформаційною безпекою; d) містить зобов'язання щодо постійного вдосконалення системи управління інформаційною безпекою. Політика інформаційної безпеки має: e) бути доступною як документована інформація;ї) бути розповсюдженою в середині організації; g) бути доступною зацікавленим сторонам, за потреби. 5.3 Організаційні ролі, відповідальності та повноваження. Вище керівництво повинно гарантувати, що відповідальності та повноваження для ролей, пов'язаних з інформаційною безпекою, призначені й доведені. Вище керівництво повинно призначити відповідальності та повноваження для: a) гарантування, що система управління інформаційною безпекою відповідає вимогам цього стандарту; b) звітування вищому керівництву щодо результативності системи управління інформаційною безпекою.		+	
6	Планування			
	6.1 Дії з розгляду ризиків та можливостей 6.1.1 Загальні положення При плануванні системи менеджменту інформаційної безпеки організація повинна враховувати фактори, зазначені в 4.1, і вимоги, наведені в 4.2, а також визначати ризики інформаційної		+	

	безпеки і можливості організації, що підлягають розгляду: a) забезпечення впевненості у тому, що система менеджменту інформаційної безпеки здатна досягти намічених результатів; b) запобігання або зменшення небажаних наслідків; c)забезпечення постійного покращення). Організація має планувати: d) дії щодо розгляду даних ризиків та можливостей; e) яким чином: 1) інтегрувати та впроваджувати ці дії у процеси системи менеджменту інформаційної безпеки; 2) оцінювати результативність цих процесів. 6.1.2 Оцінка ризиків інформаційної безпеки Організація повинна визначити та впровадити процес оцінки ризиків інформаційної безпеки, який дозволяє : a) встановлювати та підтримувати критерії ризиків інформаційної безпеки, включаючи: 1) критерії ухвалення ризиків інформаційної безпеки; 2) критерії щодо оцінки ризиків інформаційної безпеки; b) забезпечувати впевненість у тому, що повторні оцінки ризиків інформаційної безпеки дають несуперечливі, достовірні та порівняні результати; c) ідентифікувати ризики інформаційної безпеки, тобто: 1) застосовувати процес оцінки ризиків інформаційної безпеки для ідентифікації ризиків, пов'язаних з порушенням конфіденційності, цілісності та доступності інформації в рамках сфери дії системи менеджменту інформаційної безпеки; 2) ідентифікувати власників ризиків інформаційної безпеки; d) проводити аналіз ризиків інформаційної безпеки, тобто: 1) оцінювати потенційні наслідки, які можуть статися внаслідок реалізації ризиків інформаційної безпеки, ідентифікованих відповідно до 6.1.2 c) 1); 2) оцінювати реальну ймовірність реалізації ризиків інформаційної безпеки, ідентифікованих відповідно до 6.1.2 c) 1); 3) визначати рівні ризиків інформаційної безпеки; e) оцінювати ризики інформаційної безпеки, тобто: 1) порівнювати результати аналізу ризиків інформаційної безпеки з критеріями ризиків, встановленими відповідно до 6.1.2 a); 2) визначати пріоритетність обробки проаналізованих ризиків інформаційної безпеки . Організація повинна зберігати документовану інформацію про процес оцінки ризиків інформаційної безпеки. 6.1.3 Обробка ризиків інформаційної безпеки Організація повинна визначити та застосовувати процес обробки ризиків інформаційної безпеки: a) для вибору відповідних варіантів обробки ризиків інформаційної безпеки, враховуючи результати оцінки ризиків інформаційної безпеки; b) визначення всіх заходів та засобів інформаційної безпеки, необхідних для реалізації обраного(их) варіанта(ів) обробки ризиків інформаційної безпеки. c) порівняння заходів та засобів інформаційної безпеки, визначених відповідно до 6.1.3 Ь), із зазначеними у додатку А для перевірки того, що жодних необхідних заходів забезпечення інформаційної безпеки не було втрачено. d)підготовки відомості про застосування заходів та засобів інформаційної безпеки, яка містить: -необхідні заходи щодо забезпечення інформаційної безпеки; -обґрунтування їх застосування;			

	-інформацію про те, чи реалізовані необхідні заходи забезпечення інформаційної безпеки; -обґрунтування незастосування заходів та засобів інформаційної безпеки, поданих у додатку А; e)розроблення плану обробки ризиків інформаційної безпеки; f)узгодження та (або) затвердження плану обробки ризиків інформаційної безпеки та прийняття залишкових ризиків та інформаційної безпеки власниками ризиків. Організація повинна зберігати документовану інформацію про процес обробки ризиків інформаційної безпеки. 6.2 Цілі інформаційної безпеки та плани щодо їх досягнення В організації повинні бути встановлені цілі забезпечення інформаційної безпеки стосовно відповідних функцій та рівнів управління організацією. Цілі інформаційної безпеки повинні: a)бути узгоджені з політикою інформаційної безпеки; b)бути вимірними (якщо це практично можливо); c)враховувати застосовні вимоги інформаційної безпеки та результати оцінки та обробки ризиків інформаційної безпеки; d)бути доведені до відома всіх зацікавлених сторін; e)оновлюватись у міру необхідності. Організація повинна зберігати документовану інформацію про цілі інформаційної безпеки . При плануванні способів досягнення своїх цілей інформаційної безпеки організація має визначити: f)що має бути зроблено; д) які ресурси потрібні; h)хто нестиме відповідальність; i)коли запланований захід буде завершено; j)як оцінюватимуться результати.			
7	Забезпечення та підтримка			
	7.1 Ресурси забезпечити наявність ресурсів, необхідних для створення, впровадження, підтримки та постійного покращення системи менеджменту інформаційної безпеки. 7.2 Кваліфікація Організація повинна: a) визначити необхідну кваліфікацію для осіб (a), які виконують роботу під її контролем, яка впливає на забезпечення її інформаційної безпеки; b) переконатися, що кваліфікація цих осіб базується на їх прийнятній освіті, професійній підготовці (стажуванні) чи досвіді роботи; c) за необхідності вживати заходів щодо отримання необхідної кваліфікації та проводити оцінювання результативності вжитих заходів; d) зберігати відповідну документовану інформацію як свідчення наявності необхідної кваліфікації. 7.3 Поінформованість Особи, які виконують роботу під контролем організації, повинні бути обізнані: a) про політику інформаційної безпеки організації; b) їх внесок у забезпечення результативності системи менеджменту інформаційної безпеки, включаючи користь від покращення діяльності щодо забезпечення інформаційної безпеки; c) наслідки недотримання вимог системи менеджменту інформаційної безпеки. 7.4 Взаємодія			

	В організації має бути визначена необхідність у взаємодії всередині організації та із зовнішніми сторонами з питань, що мають відношення до системи менеджменту інформаційної безпеки, включаючи такі: a) предмет взаємодії; b) коли взаємодіяти; c) з ким взаємодіяти; d) хто має взаємодіяти; e) процедури здійснення взаємодії 7.5 Документована інформація 7.5.1 Загальні положення Система управління інформаційної безпеки організації повинна включати: a) документовану інформацію, необхідну відповідно до цього стандарту; b) документовану інформацію, яка визначається організацією як необхідна для забезпечення результативності системи менеджменту інформаційної безпеки. 7.5.2 Створення та оновлення документованої інформації При створенні та оновленні документованої інформації організація має забезпечити належні: a) ідентифікацію та опис (наприклад, найменування, дата, автор або номер для посилань); b) формат (наприклад, мова, версія програмного забезпечення, графіка) та носій інформації (наприклад, паперовий, електронний); c) перевірку та підтвердження її придатності та адекватності. 7.5.3 Управління документованою інформацією Потрібно здійснювати управління документованою інформацією, необхідною для системи менеджменту інформаційної безпеки та зазначеною в цьому стандарті, з метою забезпечення її: a) доступності та придатності для використання, коли і де це необхідно; b) належного захисту. Для управління документованою інформацією організація повинна здійснювати наступні (якщо це застосовно) дії щодо неї: c) поширення, забезпечення доступу, пошуку та використання; d) зберігання та забезпечення безпеки, включаючи збереження розбірливості; e) керування змінами (наприклад, керування версіями); f) архівне зберігання та знищення. Організація повинна ідентифікувати та керувати необхідною для здійснення планування та функціонування системи менеджменту інформаційної безпеки документованою інформацією із зовнішніх джерел.			
8	Функціонування			
	8.1 Оперативне планування та контроль Організація повинна планувати, реалізовувати та контролювати процеси, необхідні для відповідності вимогам інформаційної безпеки та для здійснення дій, визначених у 6.1. Організація повинна також реалізовувати плани з досягнення цілей інформаційної безпеки , визначених відповідно до 6.2. Організація повинна зберігати документовану інформацію в обсязі, необхідному для забезпечення впевненості, що процеси були виконані відповідно до планів. В організації необхідно управляти запланованими змінами системи менеджменту інформаційної безпеки та аналізувати наслідки незапланованих змін, вживаючи при необхідності заходи щодо зниження будь-		+	

	яких несприятливих наслідків. Процеси організації, які здійснюються з використанням аутсорсингу, повинні бути визначені та проконтрольовані. 8.2 Оцінка ризиків інформаційної безпеки Організація повинна проводити оцінку ризиків інформаційної безпеки через заплановані інтервали часу або у разі передбачуваних або суттєвих змін, що відбулися, враховуючи критерії ризиків інформаційної безпеки , встановлені відповідно до 6.1.2 a). Організація повинна зберігати документовану інформацію щодо результатів проведених оцінок ризиків інформаційної безпеки. 8.3 Обробка ризиків інформаційної безпеки Організація має реалізувати план обробки ризиків інформаційної безпеки. Організація повинна зберігати документовану інформацію щодо результатів обробки ризиків інформаційної безпеки.			
9	Оцінювання виконання			
	9.1 Моніторинг, оцінка захищеності, аналіз та оцінювання Організація повинна оцінювати діяльність із забезпечення інформаційної безпеки, а також результативність системи управління інформаційною безпекою. Організація має визначити: a) об'єкти моніторингу та оцінки захищеності, включаючи процеси, заходи забезпечення інформаційної безпеки; b) методи проведення моніторингу, оцінки захищеності, аналізу та оцінювання, що забезпечують впевненість у достовірності результатів. c) коли проводити моніторинг та оцінку захищеності; d) хто має здійснювати моніторинг та оцінку захищеності; e) коли аналізувати результати моніторингу та оцінки захищеності; f) хто має здійснювати аналіз та оцінювання цих результатів. Організація повинна зберігати відповідну документовану інформацію як свідчення результатів моніторингу та оцінки захищеності. 9.2 Внутрішній аудит Організація повинна через заплановані інтервали часу проводити внутрішні аудити з метою визначення, наскільки система управління інформаційною безпекою: a) відповідає: 1) власним вимогам організації до системи менеджменту інформаційної безпеки ; 2) вимогам цього стандарту; b) ефективно реалізована та підтримується. Організація повинна: c)планувати, розробляти, реалізовувати та підтримувати програму(и) аудиту, включаючи визначення періодичності та методів проведення аудиту, відповідальність, вимоги до планування та надання звітності аудиту. Програма(и) аудиту повинна(и) враховувати значущість перевірених процесів та результати попередніх аудитів; d)визначати критерії та область проведення кожного аудиту; e)вибирати аудиторів та супроводжувати проведення аудитів для забезпечення впевненості в об'єктивності та неупередженості процесу аудиту; f)забезпечувати надання результатів аудитів відповідним керівникам організації ; д) зберігати документовану інформацію як свідчення реалізації програм(и) аудиту та результатів аудиту. 9.3 Перевірка з боку керівництва		+	

	Вищий посібник повинен проводити перевірку системи менеджменту інформаційної безпеки через заплановані інтервали часу з метою забезпечення впевненості в її прийнятності, адекватності та результативності, що зберігається. Перевірка з боку керівництва повинна містити розгляд: a)стану виконання рішень за наслідками попередніх перевірок з боку керівництва; b)змін зовнішніх та внутрішніх факторів щодо системи менеджменту інформаційної безпеки; c)відгуків про результати діяльності щодо забезпечення інформаційної безпеки, включаючи тенденції та: 1)у виявленні невідповідностей та застосуванні коригувальних дій; 2)результати моніторингу та оцінки захищеності; 3)результати аудиту; 4)досягненні цілей інформаційної безпеки; d)відгуків від зацікавлених сторін; e)результатів оцінки ризиків інформаційної безпеки та статусу виконання плану обробки ризиків інформаційної безпеки; f)можливостей для постійного покращення системи менеджменту інформаційної безпеки. Результати перевірки з боку керівництва повинні включати рішення, які стосуються можливостей постійного поліпшення та необхідності внесення будь-яких змін до системи менеджменту інформаційної безпеки організації. Організація повинна зберігати документовану інформацію як свідчення результатів перевірок з боку керівництва.			
10	Вдосконалення			
	10.1 Невідповідності й корегувальні дії У разі виявлення невідповідностей організація повинна: a) реагувати на невідповідності і за можливості: 1) виконувати дії для контролю та їх корекції; 2) вживати заходів щодо наслідків; b) оцінювати потреби в діях для усунення причин невідповідностей для запобігання їх повторення чи виникнення будь-де за допомогою: 1) перегляду невідповідностей; 2) визначення причин невідповідностей; 3) визначення, чи існують подібні невідповідності або потенційно можуть з 'являтися; c) впровадити певні дії, за потреби; d) переглянути ефективність виконаних коригувальних дій; e) внести зміни до системи управління інформаційною безпекою, за потреби. Коригувальні дії мають бути адекватними до наслідків виявлених невідповідностей. Організація повинна зберігати документовану інформацію як доказ: f) сутності невідповідностей та будь-яких послідовних дій, що були виконані, g) результати будь-яких коригувальних дій. 10.2 Постійне вдосконалення. Організація повинна постійно вдосконалювати придатність, адекватність та ефективність си стеми управління інформаційною безпекою, гарантування її постійної придатності, адекватності та ефективності.		+	

9. Висновок:

В ході перевірки системи менеджменту підприємства ТОВ «ВІЕНЕРДЖІ» на відповідність вимогам ДСТУ ISO/IEC 27001:2023, яка ґрунтується на процесі вибірки доступної інформації проведення аудиту, група аудиту отримала об'єктивні дані, що засвідчують:

- система менеджменту підприємства ефективна(на підставі доказів, що відносятся до можливості системи менеджменту відповідати застосовним вимогам та очікуваним результатам; внутрішніх аудитів та процесу аналізу з боку керівництва):

☒ Так ☐ Ні

- сфера сертифікації прийнятна:

☒ Так ☐ Ні

- цілі аудиту було досягнуто:

☒ Так ☐ Ні

- підприємство здатне постійно виготовляти продукцію, яка відповідає вимогам відповідних нормативних документів:

☒ Так ☐ Ні

- підприємство має можливості для своєчасного виявлення продукції незадовільної якості:

☒ Так ☐ Ні

- підприємство вживає (не вживає) заходи щодо запобігання виготовлення такої продукції на постійній основі:

☒ Так ☐ Ні

- підприємство ефективно контролює використання документів про сертифікацію (при проведенні повторної сертифікації):

☒ Так ☐ Ні

10. Враховуючи викладене, група аудиту вважає, що система ТОВ «ВІЕНЕРДЖІ»

☒ відповідає вимогам ДСТУ ISO/IEC 27001:2023,

☐ в цілому відповідає вимогам _____ за умови усунення невідповідностей

☐ не відповідає вимогам _____

Необхідність повторної оцінки заявника на місці для підтвердження усунення невідповідностей

☐ Так ☒ Ні

і рекомендує ОС ТОВ «ТЕСТМЕТРСТАНДАРТ» видати сертифікат на систему менеджменту ДСТУ ISO/IEC 27001:2023 стосовно неспеціалізованої оптової торгівлі; оптової торгівлі побутовими електротоварами й електронною апаратурою побутового призначення для приймання, записування, відтворювання звуку й зображення, електронним і телекомунікаційним устаткованням, деталями до нього, іншими машинами й устаткуванням; роздрібної торгівлі в спеціалізованих магазинах електронною апаратурою побутового призначення для приймання, записування, відтворювання звуку й зображення; інших видів роздрібної торгівлі в неспеціалізованих магазинах та поза магазинами, роздрібної торгівлі, що здійснюється фірмами поштового замовлення або через мережу інтернет; ремонт і технічне обслуговування електронного й оптичного устаткування та електричного устаткування; ремонту електронної апаратури побутового призначення для приймання, записування, відтворювання звуку й зображення; діяльності у сфері інжинірингу, геології та геодезії, надання послуг технічного консультування в цих сфе-

рах.

☒ Так ☐ Ні

терміном до 3 –х років.

Контроль відповідності сертифікованої системи менеджменту вимогам ДСТУ ISO/IEC 27001:2023 протягом терміну дії сертифіката буде здійснюватися шляхом проведення наглядових аудитів.

Періодичність наглядового аудиту:
- першого – не пізніше ніж через 12 місяців після прийняття рішення про сертифікацію;
- другого – не пізніше ніж через 24 місяця після прийняття рішення про сертифікацію.

11. Розповсюдження звіту

Звіт складено на 11 арк. у 2 прим. і направлено (вручено):
1. ТОВ «ТЕСТМЕТРСТАНДАРТ» -1 прим.
2. ТОВ «ВІЕНЕРДЖІ»– 1 прим.

12. Вимоги конфіденційності

Інформація за матеріалами перевірки, що становить комерційну таємницю, є конфіденційною і не підлягає поширенню без письмової згоди сторін: ОС ТОВ «Тестметрстандарт» та ТОВ «ВІЕНЕРДЖІ»

Примітка: При незгоді з висновками, наведеними у даному акті, ТОВ «ВІЕНЕРДЖІ» має право подати апеляцію в апеляційну комісію ОС ТОВ «Тестметрстандарт» протягом місяця з дати отримання звіту.

Керівник групи аудиту _____ Оксана САК

Аудитор _____ Юлія ГЕРАСИМЧУК

Тех. експерт _____ Віктор ГЕРАСИМЧУК

Зі звітом ознайомлений та один примірник отримав:
Директор ТОВ «ВІЕНЕРДЖІ» _____ Андрій ШТЕПА

24.10.2023р.