מערכת Qualla

מבית קויוטי טכנולוגיות ופיתוחים בע"מ, ח.פ. 516969987 ("**קויוטי**" או "**החברה**")

מדיניות פרטיות - תנאי עיבוד מידע

1. כללי – רקע ומטרות המסמך

1.1 החברה מעמידה לרשות לקוחותיה את מערכת Qualla, מערכת מקוונת המסופקת כשירות במודל SaaS (Software as a Service). המערכת מאפשרת למשתמשים לקבל ממבטחים שונים ציטוטי מחיר לפוליסות ביטוח אלמנטרי מסוגים שונים, בכפוף לתנאי החיתום של כל מבטח. ציטוטי המחיר אינם מחייבים את המבטחים, והפקת הפוליסה כפופה להשלמת הליך החיתום ולהנפקתה על ידי המבטח (בהתאמה: "**המערכת**" ו-"**ציטוטי מחיר להצעות לביטוח**").

1.2 המערכת מועמדת לשימוש הלקוחות ולמשתמשים מטעמם, בהתאם להוראת הלקוחות. ובהתאם לתנאי השימוש ולמדיניות פרטיות זו, למשך התקופה בה רכשו רשות להשתמש בה בהתאם לתנאי השימוש.

1.3 מטרת מדיניות פרטיות זו היא לשקף טיפול החברה (לרבות עיבוד מידע, כמוגדר בהמשך, שנעשה על ידה): (1) במידע (מידע - לרבות מידע אישי) שמוזן למערכת על ידי המשתמשים בה מטעם לקוחותיה ובמידע שמתקבל מהמבטחים במענה למידע שהוזן כאמור ("**מידע הלקוח**"), לרבות פירוט העניינים שיש להסדיר בהסכם בהתאם לתקנה 15 לתקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017 ("**תקנות אבטחת מידע**"); וכן (2) במידע אודות גישה ושימושי משתמשי הלקוחות במערכת, למעט מידע הלקוח ("**מידע השימוש**").

2. צרופות מונחים ופרשנות

2.1 הצרופות למדיניות פרטיות זו מהוות חלק בלתי נפרד ממנה.

2.2 למונחים הבאים תהא המשמעות שלהלן:

2.2.1 "**המערכת**" – כהגדרת המונח בסעיף 1.1 למדיניות זו.

2.2.2 "**דיני הגנת הפרטיות**" – החוק, תקנות שהותקנו מכוחו, לרבות תקנות אבטחת מידע והנחיות הרשות להגנת הפרטיות.

2.2.3 "**מידע אישי**" - נתון הנוגע לאדם מזוהה או לאדם הניתן לזיהוי; לעניין הגדרה זו, "אדם הניתן לזיהוי" – מי שניתן לזהותו במאמץ סביר, במישרין או בעקיפין, ובכלל זה באמצעות פרט מזהה, כגון שם, מספר זהות, מזהה ביומטרי, נתוני מיקום, מזהה מקוון, או נתון אחד או יותר הנוגע למצבו הפיזי, הבריאותי, הכלכלי, החברתי או התרבותי.

2.2.4 "**עיבוד**" - כל פעולה שמבוצעת על מידע אישי, לרבות קבלתו, איסופו, אחסונו, העתקתו, עיון בו, גילויו, חשיפתו, העברתו, מסירתו או מתן גישה אליו.

2.3 למונחים במדיניות פרטיות זו שלא הוגדרו בה והוגדרו בחוק תהא המשמעות הקבועה להם בחוק.

2.4 הוראות מדיניות פרטיות זו גוברות בעניינים בהם היא עוסקת, על כל הסכם הסדר או הסכמה אחרת שבין החברה ללקוח, לרבות על כל הסכם שנערך בין הסכם מול המשתמשים במערכת מטעמו.

2.5 מתוך זהירות מובהר שבכל מקרה של סתירה בין הוראות החוק להוראות מדיניות פרטיות זו הוראות החוק גוברות.

3. השימוש במערכת והזנת מידע למערכת

3.1 הגישה למערכת היא באמצעות דפדפן והמידע שמעובד במערכת הוא בהתאם למידע שמוזן על ידי משתמשי הלקוח למערכת.

3.2 על כל לקוח למנות נציג ("**משתמש ראשי**") והוא שאחראי להקצות ולנהל הרשאות משתמשים מטעם הלקוח.

3.3 ככלל לצורך קבלת ציטוטי מחיר להצעות ביטוח אין חובה להזין למערכת מידע אישי או מידע אישי מזהה במישרין (כגון שם המבוטח, מספר זהות וכו').

3.4 המידע שמוזן למערכת הוא בהתאם לבחירת ולהחלטת משתמשי הלקוחות. בהזנת מידע למערכת על ידי מי ממשתמשי הלקוח, הלקוח מצהיר ומתחייב שהוא משתמש במידע כדין והוא רשאי להעבירו לחברה לצורך עיבודו במערכת בהתאם להוראות מדיניות פרטיות זו. הלקוח אחראי לעמוד בכל עת בכל דרישות הדין בקשר עם עיבוד מידע אישי.

3.5 המידע המוזן במערכת מועבר לחברות הביטוח על מנת לאפשר להן להעביר ציטוטי מחיר להצעות ביטוח מטעמן. ציטוטי מחיר להצעות ביטוח שמתקבלות מוצגות למשתמשי הלקוח כפי שהן מתקבלות מהמבטחים. לחברה אין כל אחריות לציטוטי המחיר.

3.6 טיפול המבטחים, במידע שנשלח אליהם באמצעות המערכת הוא בהתאם למדיניות הפרטיות של המבטחים.

3.7 המידע שמוזן על ידי משתמשי הלקוח והמידע שמתקבל מהמבטחים בתגובה יקראו ביחד להלן "מידע הלקוח".

3.8 כל משתמש לקוח יכול לראות את מידע הלקוח.

3.9 כל משתמש רשאי יכול לראות את מידע השימוש.

3.10 מידע הלקוח ומידע השימוש מאוחסנים במערכת לתקופות כמפורט בסעיף 4 להלן ונעשים בהם עיבודים כמפורט בסעיף 3 להלן.

4. שימושי החברה במידע הלקוח ובמידע השימוש

4.1 החברה משתמשת במידע הלקוח ובמידע השימוש למטרות הבאות:

4.1.1 אספקת שירותים למשתמשי הלקוחות לרבות מענה לפניות ומשלוח הודעות. בכלל זאת משלוח מידע שהוזן על ידי משתמשי הלקוחות למבטחים לצורך קבלת ציטוטי מחיר להצעות ביטוח ממבטחים והצגתם למשתמשי הלקוחות.

4.1.2 אכיפת תנאי השימוש.

4.1.3 הפקת תובנות לטיוב ולשיפור המערכת, הפקת מידע סטטי ואגרגטיבי.

4.1.4 קיום חובות לפי דין (דין – לרבות הנחיות רשות מוסמכת).

4.1.5 הגנה על אינטרס אישי כשר (כגון הליכים מנהליים או משפטיים, או הערכות לקראת הליכים כאמור).

4.1.6 הדגמת יכולת המותר.

4.1.7 שיתוף המידע עם ספקים נוספים (צד ג') לצורך קבלת שירות משלים.

4.1.8 משלוח הצעות למוצרים ביטוחיים ופיננסים משלימים, בכפוף להוראות דיוור והוראות הדין

4.2 לעניין משלוח הודעות האמור הוא בכפוף לסעיף 4.3 להלן. על שימוש בכלי בינה מלאכותית במסגרת השימוש כאמור חלות גם הוראות סעיף 4.4 להלן.

4.3 **דבר פרסומת**

4.3.1 החברה עשויה לשלוח מעת לעת (בהודעות אלקטרוניות, במסרונים, במערכות חיוג אוטומטי או בפקס), הודעות שהן בגדר 'דבר פרסומת' (כהגדרתו בסעיף 30א לחוק התקשורת (בזק ושידורים), התשמ"ב-1982), והכל בכפוף לתנאים הנדרשים לכך בדין (לרבות איסוף הסכמה או 'מסלול לקוחות') ולזכותו של הנמען להודיע על סירוב לקבלת הודעות כאמור בכל עת.

4.3.2 ככל שהחברה תשלח לך דבר פרסומת, הנך רשאי בכל עת להודיע על סירוב לקבלתן בהתאם להוראות שימסרו בגוף כל הודעה, או באמצעות פניה לחברה באחד מאמצעי הקשר שמתפרסמים באתר האינטרנט של החברה *[כמפורט מטה]*. מובהר שאין באמור למנוע מהחברה לשלוח הודעות שירות, הודעות אישיות וכיוצ"ב.

4.4 **בינה מלאכותית.**

4.4.1 ככלל ככל שיעשה על ידי החברה שימוש בכלי בינה מלאכותית הוא יעשה למטרות לעיל, לאחר אימון כלי הבינה המלאכותית, תיקוף ביצועים, ועריכת בדיקות ובקרות מקדמיות ושוטפות, תוך הקפדה על הוגנות שקיפות, יעילות, כיבוד הפרטיות ואבטחת מידע והכל בשים לב למהות השימוש ולסיכונים שבו.

4.4.2 במקרים בהם הדין יחייב הסכמה מפורשת נפרדת לשימוש מסוים בכלי בינה מלאכותית, החברה תכבד את הדין ותפעל בהתאם.

4.4.3 במקרים בהם הדין יחייב מתן זכות ביטול הסכמה (opt-out) לנושאי מידע לשימוש מסוים במידע אישי בכלי בינה מלאכותית, החברה תכבד את הדין ותודיע לנושאי מידע על זכותם זו.

4.4.4 במקרים בהם החברה תהיה מעוניינת לעבד מידע אישי בכלי בינה מלאכותית למטרות נוספות למטרות לעיל, והדין יחייב איסוף הסכמה מפורשת לכך או עמידה בתנאים נוספים או אחרים, החברה תכבד הדין ותפעל בהתאם.

5. שמירת מידע

5.1 מידע הלקוח

5.1.1 החברה שומרת את מידע הלקוח עד 90 יום מתום תקופת ההתקשרות.

5.1.2 הלקוח רשאי בכל עת להורות לחברה למחוק את מידע הלקוח מהמערכת.

5.1.3 לבקשת הלקוח החברה תאשר ללקוח בכתב מחיקת מידע הלקוח.

כל עוד מידע הלקוח לא נמחק כאמור בסעיפים 4.1.1 או 4.1.2 לעיל, החברה תאפשר ללקוחות שמעוניינים בכך לייצא את מידע הלקוח בתצורה כפי שהחברה תודיע מעת לעת.

5.2 **מידע השימוש**

5.2.1 החברה שומרת את מידע השימוש לתקופה של לפחות 24 חודשים.

5.2.2 החברה מאפשרת ללקוחות שמעוניינים בכך לייצא עותק של מידע השימוש בתצורה כפי שהחברה תודיע מעת לעת.

6. סודיות

6.1 החברה שומרת את מידע הלקוח ומידע השימוש בסודיות.

6.2 עובדי החברה חתומים על התחייבות לשמירה על סודיות מידע הלקוח ומידע השימוש, שימוש במידע הלקוח ובמידע השימוש רק כמפורט במדיניות זו וקיום נהלי האבטחה של החברה.

7. ספקי משנה

7.1 החברה משתמשת בספקים ובקבלני משנה שמספקים לה שירותים בקשר עם המערכת ("ספקי משנה"). רשימת ספקי משנה עיקריים היא כמפורט בצרופה 1, לבקשת לקוח תימסר ללקוח רשימה מפורטת. החברה עשויה לעדכן מעת לעת את ספקי המשנה.

7.2 ספקי המשנה כפופים לחובה לשמירה על סודיות, קיום נהלי אבטחת מידע ושימוש במערכת לצרכי אספקת השירותים בלבד (כולל אבטחה ותפעול השירותים), אך למעט שימוש שמתחייב לפי דין, הפקת מידע סטטיסטי אגרטיבי או אנונימי.

8. אמצעי אבטחה ואחריות החברה

8.1 החברה נוקטת אמצעי אבטחה בהתאם לתקנות אבטחת מידע, כמפורט בצרופה 2 למדיניות פרטיות זו.
8.2 החברה תהא רשאית לעדכן מעת לעת אמצעי יישום אבטחת המידע (ותמסור על כך הודעה ללקוחות) בכפוף לכך שעדכון כאמור לא יביא להפחתת אמצעי האבטחה מהנדרש לפי דיני הגנת הפרטיות.

9. דיווחים

9.1 החברה תדווח ללקוח על אירועי אבטחת מידע חמורים (כהגדרתם בתקנות אבטחת מידע) בקשר עם מידע הלקוח או מידע השימוש ותעדכן בתדירות סבירה את הלקוח בדבר אופן טיפולה בהם.

9.2 לבקשת הלקוח, אחת לשנה החברה תמסור ללקוח דיווח אודות קיום התחייבויותיה לפי מדיניות פרטיות זו.

9.3 החברה תסייע ללקוח כמיטב יכולת הסבירה ותמסור לו כל מידע בקשר עם מידע הלקוח ומידע השימוש ככל שהלקוח יידרש לכך לצרכי ביקורת של רשות מוסמכת, מענה לפניות רשות מוסמכת או צו שיפוטי.

10. ביקורת

10.1 הלקוח רשאי, אחת לשנה, לקיים על חשבונו, ביקורת בדבר קיום חיובי החברה בהתאם להוראות מדיניות זו, בכפוף לתנאים הבאים: (1) המבקר יהיה בעל הכשרה נאותה לענייניים נשוא הביקורת ועובד אחד מעשרת משרדי ראיית החשבון הגדולים בישראל; (2) המבקר יחתום על התחייבות לשמירה על סודיות; (3) הביקורת תעשה באופן שלא ישבש או יפריע לפעילות החברה; (4) הביקורת תעשה במועד שיתואם בהסכמה בין הצדדים ובלבד שמועד כאמור יהיה בתוך 21 ימי עבודה ממועד בקשת הלקוח לקיים ביקורת וקיום האמור בס"ק 1 ו-2.

11. אחריות החברה

11.1 אחריות החברה היא לקיים חיוביה כמפורט במדיניות פרטיות, בכפוף לקיום האמור החברה לא תהיה אחראית לכל נזק מכל מין וסוג שהוא שיגרם כתוצאה מהשימוש במערכת. ככל שהחברה לא תעשה כן, היא תהא אחראית לכל נזק ישיר שיגרם ללקוח גם לסך התמורה ששילם הלקוח עבור השימוש במערכת

==========

צרופה 1

שם הספק	מהות השירות	מקום אספקת השירות	עיבוד/גישה למידע	הסדרי סודיות	הסדרי אבטחה
אינמנאג' בע"מ	פיתוח תוכנה	תל אביב	מלא	DPA+NDA	ISO 27001
טלרום	שמירת כרטיסי אשראי	תל אביב	ללא גישה למערכת	DPA+NDA	PCI-DDS
AWS	אחסון ענן	האיחוד האירופי	המידע נשמר על שרתי AWS (מערכות ענן)	DPA + AWS Customer Agreement	ISO 27001

==========

צרופה 2

יישום תקנות אבטחת מידע על ידי החברה

1 כללי

1.1 צרופה זו למדיניות הפרטיות של החברה מיועדת לשקף ולפרט את האופן שבו החברה מיישמת חובות אבטחת מידע בהתאם לתקנות אבטחת מידע בקשר עם מידע שהיא מעבדת עבור לקוחותיה.

1.2 החברה בחרה ליישם את הסדרי אבטחת המידע החלים על מאגרי מידע שחלה עליהם רמת האבטחה הבינונית ביחס לכל מאגרי המידע המוחזקים על ידי קויוטי.

2 תקנה 2 - מסמך הגדרות המאגר

2.1 בהתאם לתקנה 19(א) לתקנות אבטחת מידע תקנה 2 אינה חלה על מחזיקים, על אלא רק על בעלי שליטה במאגרי המידע (כגון לקוחות החברה). בהתאם, קיום הוראות תקנה זו הוא באחריות לקוחות החברה.

3 תקנה 3 - ממונה על אבטחת מידע

3.1 החברה התקשרה עם מנהל אבטחת מידע (CISO) שאחראי על כלל נושאי אבטחת המידע בחברה לרבות המערכת, הכנת נהלי אבטחת מידע והכנת תכנית לבקרה שוטפת על עמידת החברה בדרישות התקנות.

4 תקנה 4 - נוהל אבטחה

4.1 לחברה נוהל אבטחת מידע שכולל, בין היתר:
4.1.1 הוראות בעניין האבטחה הפיזית והסביבתית של אתרי המערכת.
4.1.2 הוראות בעניין הרשאות גישה למערכת וכן, הוראות למורשי גישה כאמור.
4.1.3 תיאור של אמצעים שמטרתם הגנה על המערכת ואופן הפעלתם לצורך כך.
4.1.4 הסיכונים שחשוף להם המידע שבמערכת במסגרת הפעילות השוטפת (לרבות אלה הנובעים ממבנה המערכת), אופן קביעת סיכונים אלה, ואופן הטיפול בהם.
4.1.5 אופן ההתמודדות עם אירועי אבטחת מידע.
4.1.6 הוראות לעניין ניהול של התקנים ניידים ושימוש בהם.
4.1.7 הוראות בעניין אמצעי זיהוי ואימות לגישה למערכת.
4.1.8 הוראות לבקרה על השימוש במערכת ותיעוד גישה ושימוש במערכת.
4.1.9 הוראות לעניין ביקורות תקופתיות.
4.1.10 הוראות בעניין וידוא תקינות אמצעי אבטחה.
4.1.11 הוראות בעניין גיבוי ושחזור נתוני אבטחה.
4.1.12 הוראות לעניין פיתוח מאובטח.

[ההתייחסות היא למערכת. לברר ולהשלים ככל שיש מידע שמעובד במקומות נוספים מחוץ למערכת]

5 תקנה 5 - מיפוי מערכות המאגר

5.1 קויוטי מחזיקה במסמך מעודכן של מבנה המערכת כולל רשימת מצאי.

==========

<u>חל רק על מאגרים ברמת האבטחה הגבוהה</u>:

5.2 החברה דואגת לערוך אחת לשמונה עשר חודשים (1) סקר לאיתור סיכוני אבטחת מידע ו-(2) מבדקי חדירה לבחינת עמידות המערכת בפני סיכונים פנימיים וחיצוניים.

5.3 מבדקים אלו נערכים על ידי גופים חיצוניים מובילים בתחום אבטחת המידע. תוצאות המבדקים נבחנות בקפידה ובמידת הצורך מבוצעות פעולות מתאימות לתיקון ליקויים והמסמכים הרלוונטיים מעודכנים.

6 תקנה 6 - אבטחה פיזית וסביבתית

החברה פועלת לאבטח פיזית וסביבתית את המערכותיה (הנכללות בתקנה 5) ככל ונדרש ובהתאם לדין.

6.1 המערכת שמורה במקום מוגן למניעת חדירה וכניסה אליו ללא הרשאה.

6.2 הגישה לאתר בו מאוחסנת המערכת מבוקרת ומתועדת.

7 תקנה 7 - אבטחת מידע בניהול כוח אדם

7.1 החברה מקפידה לגייס עובדים בעלי רמה אישית ומקצועית התואמת את רגישות המידע אליה ייחשפו במהלך העבודה בחברה. לצורך כך, נוקטת החברה אמצעים סבירים המקובלים בהליכי מיון עובדים ושיבוצם.

7.2 החברה מקיימת הדרכות תקופתיות בנושאי אבטחת מידע לכל עובדיה לפחות אחת לשנה בהיקף הנדרש לצורך ביצוע תפקידם. בעלי הרשאות חדשות (לרבות עובדים חדשים) עוברים הדרכה בנושא בסמוך לכניסתם לתפקיד או לקבלת ההרשאה.

8 תקנה 8 - ניהול הרשאות גישה

8.1 החברה קובעת הרשאות גישה לעובדיה למערכת בהתאם ובמידה הנדרשת לתפקידם בלבד.

8.2 החברה מנהלת רישום מעדכון של בעלי הרשאות הגישה למערכת.

8.3 החברה בוחנת הרשאות הגישה באופן שוטף / אחת לרבעון ומוודאת באופן שוטף עדכניות רשימת מורשי הגישה.
[לוודא נוהל שעובד שעוזב או נעדר לזמן ממושך הרשאת הגישה מתבטלת]

9 תקנה 9 – זיהוי ואימות

החברה נוקטת אמצעים להבטחת גישה למערכת לבעלי הרשאה בלבד, ובהם אימות דו-שלבי (2FA), מדיניות להחלפת סיסמאות, ניטור כניסות למערכת והגבלת גישה מחו"ל.

10 תקנה 10 – בקרת ותיעוד גישה

10.1 לחברה מנגנון תיעוד אוטומטי של גישה למערכת ושימושים בה (כולל נסיונות גישה ונסיונות שימוש) ("מנגנון הבקרה"), שכולל: זהות המשתמש, תאריך ושעת הגישה או ניסיון הגישה, רכיב המערכת שאליו בוצעה הגישה או ניסיון הגישה, סוג והיקף הגישה.

10.2 מנגנון הבקרה אינו מאפשר, ככל הניתן, ביטול או שינוי של הפעלתו. במקרה של שינוי או ביטול המנגנון נשלחות התראות לממונה על אבטחת מידע של החברה ולמנהל מערכות המידע של החברה.

10.3 לחברה נוהל המסדיר בדיקה שגרתית של מנגנון הבקרה ובמידת הצורך עריכת דו"חות על בעיות שנתגלו והצעדים שננקטו בעקבותיהן.

10.4 נתוני התיעוד נשמרים למשך עשרים וארבעה חודשים.

11 תקנה 11 - תיעוד של אירועי אבטחה

11.1 לחברה מנגנון תיעוד אוטומטי של אירועי אבטחת מידע או חשש ממשי לאירועי אבטחת מידע. מנהל אבטחת המידע של החברה מתחקר כל אירוע או חשד ממשי לאירוע אבטחת מידע.

11.2 נוהל אבטחת המידע של החברה כולל, בין היתר, הוראות להתמודדות עם אירועי אבטחה, לפי חומרת האירוע ומידת רגישות המידע, לרבות לעניין ביטול הרשאות וצעדים מיידיים אחרים הנדרשים וכן לעניין דיווח לרשם וללקוחות על אירועי אבטחה ועל פעולות שננקטו בעקבותיהם, במקרים המתחייבים לפי דיני הגנת הפרטיות. מובהר שבכפוף לדין לעניין דיווח על אירוע אבטחה חמור (ככל שיהיה כזה), דיווחים יעשו ללקוח וככל שיעשו על ידי החברה הם יעשו ככל הניתן בתיאום עם הלקוח.

11.3 החברה עורכת אחת לשנה או בהתאם לצורך, דיון באירועי האבטחה במסגרתו היא בוחנת, בין היתר, את דרכי ההתמודדות עימם, הצעדים שננקטו בעקבותיהם והצורך לעדכן את נוהל אבטחת המידע שלה.

12 תקנה 12 - התקנים ניידים

12.1 החברה אוסרת על חיבור התקנים ניידים למחשבים בעלי גישה למערכת, ללא קבלת אישור פרטני מראש ובכתב של מנהל אבטחת המידע של החברה ובכפוף לנקיטת אמצעי הגנה נאותים כגון הצפנת המידע באמצעי הצפנה מקובל.

13 תקנה 13 - ניהול מאובטח ומעודכן של מערכות המאגר

13.1 החברה מקפידה על ניהול ותפעול תקין של המערכת, בהתאם לנוהגים המקובלים בהפעלת מערכות מסוג זה, לרבות ביצוע עדכונים שוטפים לרכיבי החומרה והתוכנות שנכללות בה בהתאם להוראות יצרניהן.

13.2 המערכת מופעלת תוך הפרדה לוגית עבור כל לקוח.

13.3 המערכת מופעלת בנפרד ממערכות מידע אחרות שמשמשות את החברה.

14 תקנה 14 - אבטחת תקשורת

14.1 גישת משתמשי לקוחות למערכת נעשית בגלישה. המערכת כוללת אמצעי הגנה מפני חדירה לא מורשית ומפני תוכנות המסוגלות לגרום לנזק או שיבוש למחשב או לחומר מחשב. [לפרט]

14.2 הגישה למערכת מוצפנת באמצעות SSL , כך שמידע שמוזן למערכת או מועבר ממנה מוצפן

14.3 גישת משתמשי לקוחות למערכת מחייבת זיהוי ע"י יוזר + סיסמא / OTP.

14.4 גישה מרחוק של משתמשי החברה למערכת מחייבת שימוש ב VPN או דרך IP מורשה + הגנות על גישה מרחוק של משתמשי החברה.

15 תקנה 15 - מיקור חוץ

15.1 בהתאם לתקנה 19(א) לתקנות אבטחת מידע תקנה 15(א) אינה חלה על מחזיקים, אלא רק על בעלי שליטה במאגרי המידע (כגון לקוחות החברה). בהתאם, קיום הוראות תקנה זו הוא באחריות לקוחות החברה.

15.2 הסדרי הסודיות, האבטחה והשימוש המוגבל במידע בין החברה לבין ספקי המשנה שלה הם כמפורט במדיניות הפרטיות שצרופה זו מסופחת לה.

16 תקנה 16 - ביקורות תקופתיות

16.1 החברה עורכת ביקורת בדבר עמידתה בתקנות אבטחת מידע אחת לעשרים וארבעה חודשים. הביקורת נערכת על ידי גורם בעל הכשרה מתאימה לביקורת בנושאי אבטחת מידע (CISO חיצוני). הביקורת מתועדת בדו"ח.

16.2 במסגרת הביקורת נבחנת (והדבר מתועד בדו"ח הביקורת) התאמת אמצעי האבטחה לנוהל אבטחת המידע של החברה ולתקנות אבטחת מידע. החברה דנה בדו"חות הביקורת וככל שעולה הצורך, מעדכנת את נוהל אבטחת המידע שלה בהתאם.

17 תקנה 17 - שמירת נתוני אבטחה

17.1 החברה שומרת באופן מאובטח למשך עשרים וארבעה חודשים את הנתונים הבאים:

17.1.1 נתוני בקרה ותיעוד של הכניסה והיציאה מאתרים שבהם מצויות גישה למערכות החברה.
17.1.2 רשימת הרשאות הגישה המעודכנת, וכן, תוצרי ניטור הרשימה וביצוע הבקרה עליה.
17.1.3 נתוני מנגנון הבקרה, לרבות זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה ואם הגישה אושרה או נדחתה.
17.1.4 תוצרי ניטור ותיעוד אירועי אבטחה.
17.1.5 תוצרי ניטור של חיבור מרחוק למערכות החברה.
17.1.6 תוצרי הביקורת התקופתית בנושא אבטחת מידע.

17.2 הנתונים מגובים באופן המבטיח שניתן יהיה לשחזרם למצבם המקורי.

18 תקנה 18 - גיבוי ושחזור של נתוני אבטחה

18.1 לחברה נהלים לגיבוי ושחזור הנתונים המפורטים בסעיף 17 לעיל, לרבות הסדרי הרשאה לשחזור נתונים ותיעוד הליכי שחזור (כולל: גורם מאשר, גורם מבצע ומועד השחזור).