קבוצת אשטרום

מדיניות סייבר והגנת הפרטיות

קבוצת אשטרום

קבוצת אשטרום

הינה חברת בנייה ונדל"ן אשר פועלת בתחומים מגוונים ביניהם קבלנות, תעשיה, זכיינות, יזום, פיתוח ושיווק פרויקטי מגורים, רכישה וניהול נכסים.

מרבית פעילותה העסקית של הקבוצה מנוהלת באמצעות יחידת המערך הטכנולוגי האמון על ניהול מידע עסקי רגיש וכן על מידע אישי רגיש בהם מחזיקה הקבוצה והמוגנים מתוקף חוק הגנת הפרטיות התשמ"א 1981 ותקנות הגנת הפרטיות (אבטחת מידע), תשע"ז 2017.

בהתאם, הגדירה הקבוצה מדיניות לאבטחת המידע והגנת הסייבר והפרטיות, המתייחסת להגנה על מידע בהיבטים של סודיות, שלמות וזמינות וכן לתפיסת ההגנה בהתייחסות לאיומי סייבר שונים, במטרה להגן מפני שיבוש פעילותו התקינה של המערך הטכנולוגי של הקבוצה.

הקבוצה שמה לעצמה כיעד לפתח, ליישם ולשמר רמת אבטחה לוגית ופיזית מקובלת במטרה להגן על המידע, הנכסים והתשתית הטכנולוגית שברשותה, מפני גישה לא מורשית, שיבוש, הפרעה או השבתה, והכל בכדי להבטיח את רציפותה התקינה של פעילותה העסקית ואת העמידה בהוראות החוק הרלוונטיות החלות עליה בהקשר לנושא זה.

יובהר כי מדיניות זו נועדה לספק מסגרת עבודה מקיפה להגנה על מידע של הקבוצה ושמירה על פרטיות. עם זאת, יש להדגיש כי חרף מאמציה של הקבוצה, לא ניתן להבטיח באופן מוחלט היעדר מוחלט של אירועי סייבר או הפרות פרטיות כמפורט במדיניות. האיומים בתחום הסייבר מתפתחים ומשתנים באופן תדיר, ועלולים להתרחש אירועים בלתי צפויים שאינם בשליטת הקבוצה.

הקבוצה נוקטת באמצעים סבירים ומקובלים, זאת כמפורט במדיניות זאת, על מנת למזער את הסיכונים, אך אין הבטחה כי קיום מדיניות זאת במלואה כדי למנוע לחלוטין אירועי סייבר או הפרות בתחום הפרטיות.

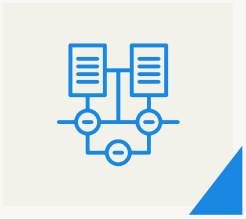
תחולה

הוראות מדיניות זו חלות על כל התהליכים העסקיים, המערכות, התשתיות, הנתונים ונכסי המידע השייכים לקבוצה, ומחייבות את כל עובדי הקבוצה וכן עובדי מיקור חוץ, קבלנים, ספקים וגורמים חיצוניים נוספים אשר קיים להם משתמש ברשת הקבוצה ו/או אשר ניגשים/מנהלים/מאחסנים מידע רגיש של הקבוצה.

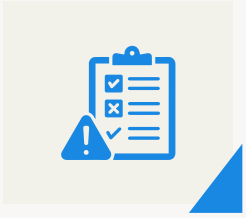
קווים מנחים ליישום המדיניות

ניהול סיכוני סייבר והגנת הפרטיות

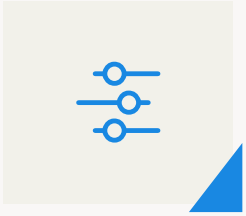
הקבוצה מנהלת את סיכוני הסייבר והגנת הפרטיות הרלוונטיים לתהליכים העסקיים, למערכות ולמידע, באופן אקטיבי, עדכני ושוטף על פי מיטב שיקול דעתה והערכתה ובהתאם לשלבים הבאים ←



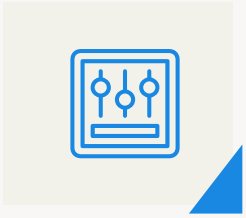
מיפוי וסיווג תהליכים, מערכות ונכסי מידע



הערכת סיכונים



ביצוע תהליכי תסקיר השפעה על פרטיות על תהליכים עסקיים ומערכות המידע



יישום בקרות וגיבוש תכנית להפחתת הסיכון

מדידה וזיהוי סיכונים באופן שוטף והערכת אמצעי ההגנה

יישום בקרות להגנת הסייבר והגנת הפרטיות

הקבוצה הגדירה ופועלת ליישום בקרות ניהוליות, תפעוליות וטכנולוגיות, במטרה לפעול להפחתת הסיכון לפגיעה בסודיות, שלמות ו/או זמינות נכסי המידע, מערכות המידע, התהליכים העסקיים ופעילותה העסקית התקינה.

הגנת סייבר הגנת המידע והגנת הפרטיות

הקבוצה הגדירה ופועלת ליישום בקרות תקופתיות למזעור סיכוני סייבר, הגנת המידע והגנת הפרטיות הנובעים מפעילות העובדים ומהפעילויות השוטפות בקבוצה. בקרות אלו הוטמעו בשלבי מחזור החיים השונים של עובד בקבוצה, החל מתהליך הגיוס (סינון, בדיקות רקע ובדיקות אמינות) ועד לשלב סיום ההעסקה.

הקבוצה גיבשה תכנית להעלאת רמת מודעות העובדים לסיכוני סייבר והגנת הפרטיות, אשר תשולב בתכנית העבודה השנתית, ותפעל להשגת המטרות הבאות:

01 העלאת רמת הידע לגבי הסייבר והפרטיות אליהם הקבוצה חשופה;

02 העלאת המודעות הארגונית הנדרשת לזיהוי ותגובה לאירועי סייבר הנובעים מאופי התפקיד.

03 הטמעת מסמכי מדיניות הגנה בסייבר והגנת הפרטיות לרבות שימוש באמצעי מחשוב, דוא"ל, ניהול סיסמאות, גלישה בטוחה ברשת האינטרנט, שימוש נאות באמצעי המחשוב של הקבוצה, וכן – ניהול מידע אישי ואחר עימו בא העובד במגע במהלך עבודתו בקבוצה. מסמכי המדיניות מסדירים בין היתר את תנאי העברת מידע אודות עובדים ו/או צדדים שלישיים, והכל לפי הוראות הדין.

הקבוצה רואה חשיבות רבה בהגנה על פרטיותם של העובדים, הדיירים, הספקים, והלקוחות. מדיניות הפרטיות שלנו כוללת התייחסות למטרות לשמן נאסף מידע מנושאי המידע, סוגי המידע הנאספים, השימושים שניתן לעשות במידע זה והדרכים בהן הקבוצה מטפלת ושומרת על מאגרי מידע אלו.

הקבוצה נוהגת בין היתר על פי עקרונות המידתיות והצמידות למטרה ביחס לשמירה על פרטיות המידע שהתקבל מצדדים שלישיים אחרים במהלך ההתקשרות בין הצדדים. בהתאם לדרישות הדין, הקבוצה גיבשה מסמכי מדיניות סייבר והגנת פרטיות ובהתאם, מנהלת ומעדכנת את מאגרי מידע, הסכמי אבטחת מידע, הסודיות והגנת הפרטיות עם ספקים ונותני שירותים ובהסכמי התקשרות ושותפות שונים, יישום מגבלות לדיווחי פרסומות ועוד מעת לעת על פי שיקול דעתה.

אבטחת מערכות, תקשורת ותפעול

קבוצת אשטרום פועלת באופן סביר ומקובל להגנת מערכות המידע, התקשורת והתפעול שלה, תוך יישום עקרונות, הנקבעים על ידי גורמי הניהול המופקדים על ניהול הסייבר והגנת הפרטיות של הקבוצה. הקבוצה פועלת באופן סביר ומקובל לשמירה על סודיות המידע, להבטחת רציפות תפקודית של מערכות המידע והפעילות העסקית, ולצמצם את הסיכונים הכרוכים בפעילות העסקית.

בקרת גישה לוגית

קבוצת אשטרום מתווה נהלים מובנים, בין היתר, לניהול בקרת הגישה הלוגית, המבוססים על עקרונות של הגנת סייבר והגנת הפרטיות מקובלים כחלק ממכלול ניהול והערכת הסיכונים. במסגרת יישום המדיניות והמסמכים הנלווים, הקבוצה נוקטת אמצעים סבירים לניהול, ניטור והגנת הזהויות. הקבוצה מוסיפה מעת לעת תהליכים פיקוח, תכנון ועדכון מסמכי המדיניות השונים, על פי מנגנוני בקרה ותיקוף שנקבעו לצורך כך.

נהלי העבודה והמסמכים הנלווים למדיניות כוללים קביעת סטנדרטים לאבטחת סיסמאות.

סקרי אבטחת מידע

קבוצת אשטרום מקיימת ככול הנדרש על פי שיקול דעתה הסביר סקרים בנושא אבטחת מידע הכוללים בין היתר:

- מיפוי וסיווג תהליכים, מערכות ונכסי מידע
- מיפוי והערכת סיכונים
- ביצוע תסקירי השפעה על פרטיות בתהליכים עסקיים ומערכות מידע
- יישום בקרות וגיבוש תכנית להפחתת הסיכון
- מדידה, ניטור שוטף וזיהוי סיכונים, והערכת אפקטיביות אמצעי ההגנה

מבדקי חדירות

קבוצת אשטרום פועלת בהתאם למדיניות אסטרטגית לביצוע מבדקי אבטחת מידע ומבדקי חדירה, אשר נועדו לבחון את קיומן ויעילותן של יישום בקרות האבטחה במערכות ובתהליכים השונים.

הגדרת הסקרים, ניהולם והתאמתם מובלת על-ידי מנהל הסייבר והגנת הפרטיות, תוך קידום עמידה בדרישות רגולטוריות וסטנדרטים מקובלים בתחום.

תכנית הטיפול, היישום והמעקב אחר ממצאי הסקרים תתעדכן ותנוהל על ידי מנהל תחום התשתיות ואבטחת המידע בתיאום עם מנהל אגף מערכות מידע, ותכלול התייחסות להיבטים השונים הנדרשים ליישום התיקונים על פי שיקול דעתם , לוחות זמנים בהתאם לרמת הסיכון, ונהלים שונים הנדרשים להחלטה בדבר אופן הטיפול או אי-הטיפול בממצאים שנחשפו, בהתאם לאילוצים עסקיים, אילוצי משאבים ותיאבון הסיכון הארגוני.

ניטור ובקרת מערכות מידע

קבוצת אשטרום פועלת ליישום תהליכי ניטור ובקרה מתקדמים לניהול ומעקב אחר אירועי סייבר במערכות מידע שונות של הארגון, במטרה לסייע בזיהוי מוקדם של איומים ואירועים, תוך ניתוח של נתוני מערכות מידע והתאמת תגובות בהתאם לצרכי הארגון, תוך שימוש במערכות ניטור המספקות תמונת מצב עדכנית בזמן אמת. זאת, באמצעות שירות מנוהל המאויש 24/7, האחראי לפיקוח ולניהול פעולות הניטור, ולסיוע בהגדרת תגובות מותאמות לאירועים, בהתאם למדיניות שנקבעה.

אבטחה פיזית וסביבתית

קבוצת אשטרום מיישמת פעולות סבירות ומקובלות מגוונות בתחום האבטחה הפיזית והסביבתית, במטרה להגן על מערכות המידע ועל המידע המאוחסן בהן מפני גישה לא מורשית, נזקים פיזיים, או הפרעות לפעילותן התקינה. בקרות אבטחה אלו נועדו לספק הגנה פיזית נאותה על הנכסים הקריטיים של הקבוצה באמצעות הגדרה ויישום אמצעי הגנה ובקרות פיזיות הכוללים מנגנוני גישה, ניהול ותיעוד בקרות גישה לאזורים רגישים.

היערכות לאירועי אבטחת מידע וסייבר

01 קבוצת אשטרום מגבשת, מעדכנת ומקדמת יישום של נהלים והוראות לניהול אירועי אבטחת מידע וסייבר, שנועדו להבטיח מענה אפקטיבי ככול הניתן ומבוקר לתרחישי אירועי סייבר ופרטיות מרכזיים.

02 אלו כוללים את אופן התגובה ודרכי הפעולה להתמודדות עם תרחישי סייבר שונים, כולל מתכונת הדיווח ותדירותו, וכן אופן ההתקשרות עם הגורמים הפנימיים והחיצוניים הרלוונטיים.

03 המדיניות מתמקדת בניהול אירועים תוך חלוקה עקרונית לשלבים, לרבות:

- גילוי
- הערכת מצב
- הכלה וניסיונות בלימה
- קידום פעולות התאוששות
- קידום חזרה לשגרה
- קיום תחקיר

הקבוצה מקיימת תרגולים תקופתיים למערכים שונים, במטרה לבחון את יעילות ההיערכות לאירועי סייבר וליישם תיקונים ושיפורים מוצעים בהתאם לממצאי תחקיר התרגול והפקת הלקחים, לרבות בתחומי הגיבוי, השרידות, היתירות, ההתנהלות בזמן אסון ותהליכי ההתאוששות מאסון כחלק מתפיסת חוסן סייבר ארגוני. כמו כן, הקבוצה מובילה תיקוף ועדכון של התוכניות בהתאם לצרכים המתעוררים, בפיקוח והנחייה של מנהל הסייבר והגנת הפרטיות.

קידום אבטחת מידע , הגנה בסייבר והגנת הפרטיות בתהליכי רכש והתקשרויות

קבוצת אשטרום פועלת ליישום עקרונות אבטחת מידע, הגנה בסייבר והגנת הפרטיות במסגרת התקשרויות מהותיות ומרכזיות עם שותפים עסקיים, ספקים וגורמים חיצוניים לאורך תהליכי הרכש וההתקשרות.

במסגרת זו, הקבוצה מסדירה בהסכמים את דרישות אבטחת המידע והפרטיות, לרבות בקרות מסוגים שונים. גורם חיצוני שנחשף למידע רגיש נדרש לחתום על הסכמי סודיות כתנאי מקדים להתקשרות.

הטמעת המדיניות

תהליך ההטמעה כולל תקשורת פנים-ארגונית סדורה, הדרכות ייעודיות לעובדים על המדיניות והנהלים הנלווים, וכן קיום פעילויות ייעודיות למניעת אירועי אבטחת מידע בפועל.

חלק מרכזי ביישום המדיניות, הנהלים ונהלי העבודה ברמות השונות, הינם בעלי התפקידים המוסמכים, כפי שהוגדרו במסמך זה.

עיקרי ממשל תאגידי תפקידים – סמכות ואחריות:

01 **הדירקטוריון:** אמון על הפיקוח בדבר ציות הקבוצה לדיני הגנת הפרטיות, לרבות פיקוח על:

- תכנית סקירה, אכיפה ובקרה פנימית אפקטיבית
- דיון במסמכי הגדרות המאגרים
- דיון בעקרונות המרכזיים של נהלי אבטחת המידע של הקבוצה
- דיון בתוצאות סקר סיכונים ומבדקי חדירות, לרבות בפעולות הנדרשות לתיקון הליקויים שהתגלו
- דיון רבעוני או שנתי (לפי עניין) באירועי אבטחת מידע שהתרחשו בארגון
- דיון בתוצאות הביקורת התקופתית שיש לקיימה אחת לשנתיים בנוגע לעמידה בתקנות

02 **מנהל מערכות מידע** אחראי על הפעילות בתחום טכנולוגיות המידע בקבוצה, ניהול נכסי הטכנולוגיות והמידע והתהליכים העסקיים הנתמכים במערכות אלו. אחראי על יישום מדיניות הגנת הסייבר, הגנת הפרטיות ונהלי אבטחת המידע, לרבות ההוראות, ההנחיות והמסמכים הנלווים, ובכלל זה – התקנה, ניהול, תפעול ותחזוקה של מוצרי הגנת הסייבר, הניטור, הגיבוי, התקשורת, טכנולוגיות המידע ותשתיות המחשוב בקבוצה, לצד אחריות על ביצוע תהליכים שוטפים לטיפול בחשיפות וחולשות אבטחת מידע וסייבר.

03 **מנהל סייבר והגנת הפרטיות משמש כממונה על הגנת הפרטיות בקבוצה.** משמש כסמכות מקצועית ומוקד ידע המעורב בכל מחזור החיים של תהליכי עבוד המידע בקבוצה ופועל להבטחת קיום הוראות חוק הגנת הפרטיות והתקנות החלות על הקבוצה. יגיש אחת לשנה דו"ח שנתי על פעילותו בנושא הפרטיות. מנהל הסייבר והגנת הפרטיות לא ימלא תפקיד נוסף או כפוף לנושא משרה אם אלו עלולים להעמידו בחשש למילוי תפקידו במפורט במסמך מדיניות הסייבר והגנת הפרטיות המלא של הקבוצה, יבצע תסקירי השפעה על פרטיות לתהליכים עסקיים וטכנולוגיות המידע של הקבוצה ופקח על ביצוע סקרי סיכוני פגיעה בפרטיות.

04 **מנהלי המאגרים** ייקימו חובתם למילוי דרישות חוק ותקנות הגנת הפרטיות, ווידוא ציות למסמכי המדיניות והנהלים של הקבוצה ביחס למאגרי המידע שתחת ניהולם, וקיום בקרה תקופתית, שוטפת ואפקטיבית אחר יישום המלצות ותיקון ממצאי סקרי הסיכונים ומבדקי החדירות התקופתיים.

דיווח אודות פעילותנו בתחום מתפרסם בדוח ה- ESG של הקבוצה.

אנו מזמינים את מחזיקי העניין שלנו לשלוח משוב, הצעות ורעיונות בתחום לכתובת:
privacy@ashtrom.co.il

כללי: מדיניות זו כתובה בלשון זכר רק מטעמי נוחות ויש לראות בכתוב כמתייחס גם ללשון נקבה