קבוצת אשטרום

מדיניות אבטחת מידע והגנת הסייבר והפרטיות

קבוצת אשטרום

קבוצת אשטרום

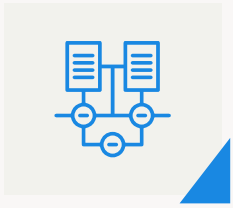
הינה חברת בנייה ונדל"ן אשר פועלת בתחומים מגוונים ביניהם קבלנות, תעשיה, זכיינות, יזום, פיתוח ושיווק פרויקטי מגורים, רכישה וניהול נכסים.

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 עליו מתבססת הקבוצה.

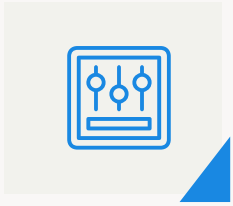
הקבוצה שמה לעצמה כיעד לפתח, ליישם ולשמר רמת אבטחה לוגית ופיזית מקובלת במטרה להגן על המידע, הנכסים והתשתית הטכנולוגית שברשותה, מפני גישה לא מורשית, שיבוש, הפרעה או השבתה, והכל בכדי להבטיח את רציפותה התקינה של פעילותה העסקית ואת העמידה בהוראות החוק הרלוונטיות החלות עליה בהקשר לנושא זה.

תחולה

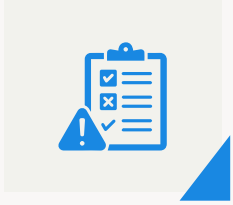
הוראות מדיניות זו חלות על כל התהליכים העסקיים, המערכות, התשתיות, הנתונים ונכסי המידע השייכים לקבוצה, ומחייבות את כל עובדי הקבוצה וכן עובדי מיקור חוץ, קבלנים, ספקים וגורמים חיצוניים נוספים אשר קיים להם משתמש ברשת הקבוצה ו/או אשר ניגשים/מנהלים/מאחסנים מידע רגיש של הקבוצה.



מיפוי וסיווג תהליכים, מערכות ונכסי מידע



יישום בקרות וגיבוש תכנית להפחתת הסיכון



הערכת סיכונים

מדידה וזיהוי סיכונים באופן שוטף והערכת אמצעי ההגנה

קווים מנחים ליישום המדיניות

ניהול סיכוני אבטחת מידע וסייבר

הקבוצה מנהלת את סיכוני אבטחת המידע והסייבר הרלוונטיים לתהליכים העסקיים, למערכות ולמידע, באופן אקטיבי, עדכני ושוטף ובהתאם לשלבים הבאים ←

יישום בקרות לאבטחת מידע ופרטיות

הקבוצה הגדירה ומיישמת בקרות ניהוליות, תפעוליות וטכנולוגיות, במטרה להפחית את הסיכון לפגיעה בסודיות, שלמות ו/או זמינות נכסי המידע, מערכות המידע, התהליכים העסקיים ופעילותה העסקית התקינה.

קבוצת אשטרום

אבטחת מידע ופרטיות

הקבוצה הגדירה ומיישמת בקרות תקופתיות למזעור סיכוני אבטחת מידע הנובעים מפעילות העובדים. בקרות אלו הוטמעו בכל שלבי מחזור החיים של עובד בקבוצה, החל מתהליך הגיוס (סינון, בדיקות רקע ובדיקות אמינות) ועד לשלב סיום ההעסקה.

הקבוצה גיבשה תכנית להעלאת רמת מודעות העובדים לסיכוני אבטחת מידע וסייבר, אשר תשולב בתכנית העבודה השנתית, תותאם לאוכלוסיות העובדים השונות, לרבות עובדי מיקור חוץ וסוכני שטח, ותפעל להשגת המטרות הבאות:

01 העלאת רמת הידע לגבי סיכוני אבטחת מידע וסייבר אליהם הקבוצה חשופה

02 העלאת המודעות הארגונית הנדרשת לזיהוי ותגובה לאירועי סייבר הנובעים מאופי התפקיד וכן, בקשה מהעובדים לאישור מדיניות הפרטיות של הקבוצה

03 הטמעת נהלי אבטחת מידע והגנת הסייבר והדרכה פרטנית בנושא הנהלים הרלוונטיים לאוכלוסיית עובדים לרבות שימוש באמצעי מחשוב, דוא"ל, ניהול סיסמאות וכן – ניהול מידע אישי ואחר עימו בא העובד במגע במהלך עבודתו בקבוצה. הנהלים מסדירים את תנאי העברת מידע אודות עובדים ו/או צדדים שלישיים, והכל לפי הנחיות החוק.

הקבוצה רואה חשיבות רבה בהגנה על פרטיותם של עובדיה. מדיניות הפרטיות שלנו כוללת התייחסות למטרות לשמן נאסף מידע מהעובדים, סוגי המידע הנאספים, השימושים שניתן לעשות במידע זה והדרכים בהן הקבוצה מטפלת ושומרת על מאגר מידע זה. המידע הנאסף ומנוהל בקבוצה הינו בעל שימושים רבים לטובת העובדים והקבוצה כאשר המרכזיים שבהם הינם:

01 ניהול משאבי האנוש של הקבוצה והשירותים הניתנים לעובדים

02 הגנה מפני דליפה של סודות מסחריים, הגנה על הקניין הרוחני וזכויות היוצרים של אשטרום והאינטרסים שלה

03 ניהול הפעילות העסקית של הקבוצה בהתאם למסמכי המדיניות ונהליה.

הקבוצה נוהגת על פי עקרונות אלו גם לגבי שמירה על פרטיות המידע שהתקבל מצדדים שלישיים אחרים במהלך ההתקשרות בין הצדדים. בהתאם לדרישות החוק, גיבשנו נהלי פרטיות ואבטחת מידע ובהתאם, מבצעת רישום ועדכון מאגרי מידע, הסכמי אבטחת מידע עם ספקים ובהסכמי התקשרות שונים, יישום מגבלות לדיווחי פרסומות ועוד. כל זאת בנוסף לפעילות שתוארה להלן לגבי הגנת פרטיות העובדים והדרכות נרחבות בתחום

ניהול סיכוני אבטחת מידע וסייבר

אבטחת מערכות, תקשורת ותפעול הקבוצה פועלת למימוש בקרות בנושא אבטחת מערכות, תקשורת ותפעול, במטרה להגן על שלמות ואמינות המידע, שמירה על רציפות תפקודית ותקינות מערכות המידע, התשתית התומכת והפעילות העסקית, עצירת התפשטות התקפות והבטחת יכולת לשחזור מערכות והתאוששות תוך מזעור הנזק שנגרם.

בקרת גישה לוגית

הקבוצה הגדירה נהלים עבור התהליכים השונים במחזור ניהול חיי משתמש לרבות יצירת חשבון משתמש, ניהול ושינוי הרשאות ונעילת חשבון ועוד. הנהלים כוללים התייחסות לאופן הביצוע, מסירת אמצעי הזדהות,

גורמים אחראיים ליישום, גורמים מוסכמים לאישור, תהליכי סקירה תקופתיים ובקרות נוספות.

סיסמאות הגישה תעמודנה בסטנדרטי אבטחה מקובלים, הקבוצה הגדירה מדיניות סיסמאות אשר תכלול מספר תווים מינימלי, מורכבות נדרשת, תדירות החלפת הסיסמא וכללים לשימוש ושמירת הסיסמא.

סקרי אבטחת מידע

הקבוצה גיבשה תכנית לביצוע סקרים ומבדקי חדירה שיבחנו את קיומן ויעילותן של בקרות ההגנה בתהליכים ובמערכות, תוך כיסוי כלל רמות האבטחה, לרבות ברמה התשתיתית, האפליקטיבית, הלוגית והסביבתית.

מנהל התחום יעדכן וינהל את תכנית הטיפול והמעקב אחר ממצאי הסקרים, אשר תכלול התייחסות לגורמים האחראיים ליישום התיקונים, לוחות זמנים בהתאם לרמת החשיפה ואופן הטיפול ו/או אי הטיפול בממצאים.

ניטור ובקרת מערכות מידע

הקבוצה מיישמת חיווי ובקרה לניטור אירועי סייבר במערכות המידע.

אבטחה פיזית וסביבתית

הקבוצה פועלת למימוש בקרות אבטחה סביבתיות במטרה למנוע גישה לא מורשית, נזק ו/או הפרעה למידע ולמערכות. במסגרת זו הוגדרו אמצעי הגנה ובקרות תוך התייחסות לבקרות גישה פיזית נדרשות בהתאם לרגישות האזורים ולניהול, שמירה והשמדת ציוד וניירת.

היערכות לאירועי אבטחת מידע וסייבר

הקבוצה הגדירה נהלים והוראות (Play Books) לניהול אירועי אבטחת מידע וסייבר, אשר מפרטים את אופן התגובה ודרכי פעולה לניהול תרחישי סייבר שונים, מתכונת ותדירות דיווח על אירועים ואופן התקשרות עם גורמים פנימיים וחיצוניים, תוך התייחסות לכל אחד משלבי ניהול האירוע: גילוי ← הערכת מצב ← הכלה ובלימה ← התאוששות ← השבה לשגרה

הקבוצה מקיימת תרגולים תקופתיים של כלל המערכים הרלוונטיים, במטרה לבחון את יעילות תכנית ההיערכות ויישום תיקונים ושינויים לשיפור בהתאם לממצאי התרגול והפקת הלקחים. כמו כן, הקבוצה תרענן מעת לעת את תכניותיה אלה.

קידום אבטחת מידע ופרטיות לכל אורך שרשרת הערך שלנו

אנו מעודדים יישום העקרונות המנחים המפורטים במדיניות זו לכל אורך שרשרת הערך שלנו ומתקשרים את חשיבות הנושא לשותפינו העסקיים, ספקינו וגורמים נוספים עימם אנו עושים עסקים. אנו רואים בכך התנהלות עסקית הוגנת וישרה המבטיחה את כל הצדדים המעורבים בהתקשרות, לצד ציות לכללי הרגולציה הקיימים בתחום. אנו מסדירים את הנושא בעת ההתקשרות עימנו.

בקרות אבטחת מידע בנושאי מיקור חוץ וניהול ספקים:

הקבוצה הגדירה נוהל המסדיר את תהליך ההתקשרות למול גורמי חוץ בהיבטי אבטחת מידע ופרטיות. במסגרת הנוהל הוגדרו הבקרות הרלוונטיות לתהליך התקשרות עם גורם חיצוני ביחס לסיכוני מיקור חוץ ואבטחת שרשרת האספקה וכן, מעורבותו הנדרשת של מנהל התחום בתהליך.

כל תהליך התקשרות למול גורם חיצוני, לרבות רכישת שירותי IT חיצוניים וביניהם שימוש בשירותים מבוססים ענן, יערך תוך שילוב דרישות והיבטי אבטחת מידע.

בנוסף, הקבוצה הגדירה נוהל לקביעת התנאים ואופן אספקת שירותי תחזוקה מרחוק על ידי נותן שירות חיצוני.

כל גורם חיצוני אשר במסגרת התקשרותו עם הקבוצה עשוי להיחשף למידע רגיש, נדרש לחתום על הסכם

סודיות והגבלות אבטחה נוספות שתקבענה בהתאם לאופי השירות אותו הוא מספק ולאופן שבו הוא ניגש/ מקבל את המידע. הנ"ל יהווה תנאי מקדים להתקשרות עמו.

הטמעת המדיניות

מדיניות זו מהווה תשתית למגוון מהלכים המבוצעים בקבוצה להבטחת יישום והטמעה מלאה החל מתקשורת פנים ארגונית, הדרכות אודות המדיניות ונהלים נלווים וכן, עריכת פעילות ייעודית למניעת אירועים בפועל.

ממשל תאגידי ליישום המדיניות – תפקידים ותחומי אחריות

- מנהל סייבר והגנת הפרטיות: הקבוצה מינתה מנהל ייעודי אשר אחראי על הגנת הסייבר והגנת הפרטיות, יקבע ויעדכן נהלי עבודה, יפעל להעלאת מודעות העובדים וליישום עקרונות ומדיניות הקבוצה בתחום זה.
- ועדת היגוי לניהול סיכוני אבטחת מידע וסייבר: הקבוצה הקימה ועדת היגוי ייעודית המתכנסת אחת לחצי שנה והינה אחראית לפיקוח והתוויות מדיניות בכל הקשור לניהולו התקין של תחום אבטחת המידע בהתאם לסיכונים, מדיניות, הוראות חיצוניות ופנימיות וצורכי הקבוצה.
- הנהלת קבוצת אשטרום: אמונה על פיקוח אודות מסגרת ניהול אבטחת המידע ואופן יישומה, מקיימת דיון שנתי בנושא ניהול סיכוני אבטחת מידע ותכנית העבודה השנתית בתחום אבטחת מידע והגנת הסייבר.

פרסום ותקשור המדיניות

מדיניות קבוצת אשטרום לקידום אבטחת מידע והגנת הסייבר והפרטיות זמינה לכלל מחזיקי העניין באתר האינטרנט של הקבוצה.

דיווח אודות פעילותנו בתחום מתפרסם בדו"ח ה- ESG של הקבוצה.

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

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