מדיניות הגנת הסייבר בבנק הפועלים – תקציר לצדדים שלישיים

2026

בנק הפועלים

מדיניות הגנת הסייבר בבנק הפועלים – תקציר לצדדים שלישיים

בנק הפועלים רואה בהגנת הסייבר יעד אסטרטגי ראשון במעלה – לא רק לשמירה על הבנק, אלא גם על לקוחותיו, עובדיו וכל השותפים העסקיים, כולל ספקי הבנק. אנו פועלים בסביבה דיגיטלית מאתגרת, בה איומי הסייבר מתפתחים ומשתנים במהירות, ולכן מחויבים למדיניות הגנת סייבר מקצועית ואפקטיבית. הגנת הסייבר היא מאפשר מהותי להתקדמות העסקית והטכנולוגית של הבנק.

יעדי הגנת הסייבר

1. **לשמור על יציבות הבנק ותפקודו** מול איומי סייבר.
2. **להגן על מידע** – בנקאי, אישי וטכנולוגי – של הבנק, העובדים, הספקים והלקוחות.
3. **לתמוך בחדשנות עסקית וטכנולוגית ובזמינות שירותי הבנק**, תוך שמירה על רמת הגנה גבוהה.
4. **לעמוד בדרישות רגולציה** ולשמור על אמון כל בעלי העניין.

עקרונות מרכזיים

1. **תשתית הגנה חזקה ומתקדמת** – מבוססת טכנולוגיות, ארכיטקטורה, תפיסות ואנשים, בהובלת מערך הגנת הסייבר, ובגישה מוכוונת סיכון – כדי להבטיח יסודות הגנה ברמה גבוהה על כלל תשתיות הבנק, כולל ענן, רשתות פנימיות, נקודות קצה ויישומים.
2. **תהליכי הגנה איכותיים ויעילים** - תכנון, הטמעה ובקרה של תהליכי הגנה ובקרות סדורות, תעדוף איומים, עמידה בתקנים ובחינה מתמדת של האפקטיביות.
3. **שותפות רוחבית** – הגנת הסייבר היא אחריות של כל גורם – הבנק, העובדים וצדדים שלישיים. כל אחד הוא חוליה קריטית בשרשרת ההגנה.

עקרונות יסוד להגנה טכנולוגית

1. **הגנה לעומק**: פריסת אמצעי הגנה טכנולוגיים להגנה במספר שכבות על כלל נכסי ה-IT של הבנק ומידע הבנק.
2. **דגש להגנת נכסי הבנק מחוץ לרשת**: דגש מיוחד יינתן למענה טכנולוגי להגנה על ערוצים ישירים המשמשים את הלקוחות, עבודת העובדים מרחוק והחיבור לצדדי ג'.
3. **מיצוי מיטבי של יכולות**: שימוש בטכנולוגיות המובילות בשוק, שילוב אוטומציה, בינה מלאכותית ויכולות זיהוי וניטור מתקדמות.
4. **התאמת ההגנה לסביבת העבודה**: חציצה מבוקרת בין מערכות הבנק לספקים, הצפנה של ערוצי מידע רגישים, הקשחת הרשאות וגישה לפי עקרון הצורך לדעת (Need to Know) והפרדת סמכויות (Separation of Duties).
5. **יישומי הגנה מתקדמים**: שילוב מערכות הגנה חכמות בארכיטקטורת ה-IT.
6. **שילוב הגנה בחדשנות**: הטמעת היבטי הגנה בתהליכי חדשנות עסקית וטכנולוגית.

מדיניות הגנת הסייבר בבנק הפועלים – תקציר לצדדים שלישיים

מאמצי הסייבר בבנק – מה אנחנו עושים בפועל?

1. **ניהול שיטתי של סיכוני סייבר** – איתור, סיווג ומיפוי נכסים קריטיים וקביעת דרך ההגנה עליהם; קיום מעגל תכנון שנתי למאמצי וטכנולוגיות ההגנה; שותפות עם בעלי העניין בבנק ומחוץ לו; עמידה דרישות ברגולציה (בדגש על נב"ת 364 החדש), בהסמכות ובתקנים מובילים; תהליכי בקרה שוטפים ורציפים; ומניעת דלף מידע.
2. **פיתוח מאובטח** - הנחייה וליווי פרויקטים, יישום בקרות הגנה בתהליכי פיתוח, בדיקות חוסן.
3. **ניהול ההגנה לכל אורך חיי המערכת** - ניהול משתמשים והרשאות, ניהול חשיפות, ביצוע סקרים ומבדקי חדירה וגריטה סדורה.
4. **מודעות ואחריות אישית** – הכשרות והדרכות מתעדכנות בהתאם לטכנולוגיות המידע ופוטנציאל האיום, חתימות על נהלי סייבר, אכיפה על חריגות, טיפול באירועים משמעתיים תוך ליווי העובד לכל אורך העסקתו בבנק מקליטה ועד עזיבה.
5. **היבטי ביטחון פיזי** – מניעת חיבור ציוד לא תקני לרשת הבנק והגנה על אתרי המחשוב וחדרי המחשוב ואזורי העבודה הרגישים בהיבטי הגנת סייבר.
6. **התמודדות עם אירועי סייבר** – איסוף מודיעין רלבנטי, ניטור מתקדם (SOC 24/7), זיהוי, ניתוח ותגובה לאירועים בזמן אמת, איסוף לוגים, שימוש במערכות מתקדמות, צוות אדום ומוכנות להמשכיות עסקית והתאוששות בקרות אירוע.
7. **עבודה עם צדדים שלישיים** – תהליכי סיווג, בקרה תקופתית, הטמעת נהלים, דיווחים בזמן אמת, והבטחת עמידה בדרישות הביטחון המוגדרות.

עקרון האחריות האישית – גם עבורכם

בבנק הפועלים, כל עובד, כל ספק וכל צד שלישי מחויב באחריות אישית להגנה על המידע אליו נחשף. הספק והצד השלישי:

1. ישמור על סודיות מידע חסוי, תוך מניעת חשיפתו לגורמים לא מורשים.
2. יעשה שימוש נאות במערכות המידע של הבנק ויקפיד על נהלי אבטחת מידע.
3. יעשה שימוש באמצעי הגנה טכנולוגיים מתקדמים ומערכות מוקשחות.
4. יוודא מתן גישה פיזית למערכות הבנק ולמידע הבנק לגורמים מורשים בלבד וחיבור ציוד מורשה בלבד.
5. ידווח באופן מיידי על אירועי אבטחת מידע או חשד לאירוע, לכלל הגורמים המוסמכים בבנק,
בדגש על מרכז אירועי אבטחת מידע הפעיל 24/7 (טלפון 03-7145511, תיבת דואר מרכז ארועי אבטחת מידע soc@poalim.co.il).

לסיכום

הגנת הסייבר היא תנאי יסוד לעבודה עם בנק הפועלים. אנו מצפים מכל ספק וצד שלישי להפגין מחויבות, מקצועיות ושקיפות מלאה – לטובת הבנק, לקוחותיו, וגם לטובתכם.

הקפדה על מדיניות הסייבר היא לא רק דרישה טכנית – אלא ערך מקצועי, עסקי ואתי.

יחד, נבטיח שותפות בטוחה ואמינה ועמידה באתגרים של העולם הדיגיטלי.

צוות הגנת הסייבר של בנק הפועלים עומד לשירותכם – לשאלות, הדרכות, או הבהרות

בנק הפועלים