מאיירס-ג'וינט-ברוקדייל
MYERS-JDC-BROOKDALE
مايرس - جوينت - بروكديل

אבטחת מידע והגנה על הפרטיות

עשה ואל תעשה אחריות אישית

>> רקע ומטרות

חברות וארגונים נושאים באחריות לשמירת החיסיון, הסודיות והפרטיות של לקוחותיהם. בשנים האחרונות אנו עדים לפגיעה כלכלית ותדמיתית של חברות וארגונים אשר נגרמת מחשיפת מידע רגיש על לקוחותיהם. מידע רגיש כולל מספר זהות, שם פרטי ושם משפחה, כתובת מגורים, מידע רפואי, מצב כלכלי, דעות פוליטיות, נטייה מינית, עבר פלילי ועוד.

גם מכון ברוקדייל וכל עובדיו מחוייבים להגן על מאגרי המידע במכון, במסגרת החוק להגנת הפרטיות ולתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז 2017. מטרת המסמך הזה היא להציג הנחיות הנגזרות מחובתנו כעובדי המכון. בהמשך יובא מסמך נוסף שיציג את דרכי הטיפול בקובצי מידע חיצוניים המגיעים למכון, קליטתם והשימוש בהם לאורך חיי המחקר.

>> שמירת סודיות

- יש לשמור על סודיות המידע והנתונים שאליהם הוא נחשף במהלך עבודתו.
- יש להימנע מחשיפת מידע חסוי, שאינו נדרש לשם ביצוע העבודה, לגורם חיצוני או לגורם פנימי.
- יש לשמור מידע חסוי במערכות הארגוניות המיועדות לכך בלבד. חל איסור לשמור מידע חסוי בכונן מקומי C או בכוננים חיצוניים כגון התקן נתיק (Disk-on-key).

>> שם משתמש וסיסמה

- שם המשתמש והסיסמה למערכות הממוחשבות ולמחשבי הארגון הם אישיים ונועדו לשימוש אישי בלבד. חל איסור למסור פרטים אלו לידי כל גורם אחר.
- חל איסור לשמור סיסמה במקום שבו היא עלולה להיחשף.
- בכל מקרה של חשיפת סיסמה או חשד לחשיפתה, יש להחליף את הסיסמה מיידית ולדווח לצוות התמיכה.

>> התקנה והסרה של תוכנות

- חל איסור מוחלט להתקין במחשבי הארגון תוכנות כלשהן.
- אם עולה הצורך להתקין תוכנה לצורכי עבודה, יש לפנות אל צוות התמיכה.
- חל איסור להשבית או להסיר תוכנות אבטחה כגון אנטי-וירוס, Firewall וכו', שהותקנו במחשבי הארגון על ידי צוות התמיכה.

>> כללי השימוש באינטרנט

- שימוש ברשתות חברתיות לצרכים ארגוניים, כגון העלאת תכנים ל-Youtube, פתיחה של פלטפורמת Facebook רשמית מטעם הארגון וכד', מחייבים אישור מקדים של Marcom ו/או של דוברות ג'וינט ישראל.
- ככלל, חל איסור להציג דעה אישית כמייצגת את עמדת הארגון ברשתות החברתיות.
- חל איסור להעביר/לשמור/לסנכרן מידע ארגוני באמצעות מגוון היישומים הקיימים באינטרנט (כגון iCloud, Google Docs/Drive וכדומה) שאינם מורשים לשימוש הארגון.
- יש להימנע מגישה למידע חסוי או ממסירה של שם משתמש וסיסמה בעת החיבור לרשת אינטרנט אלחוטית (Wi-Fi) במקומות ציבוריים, כגון בתי מלון, שדות תעופה ובתי קפה.
- יש לנקוט אמצעי זהירות סבירים בעת הגלישה באינטרנט, לרבות הימנעות מלחיצה על פרסומות, חלונות קופצים וקישורים לא מאובטחים העשויים להדביק בווירוסים ובתוכנות זדוניות.
- חל איסור להשתמש במחשב הניתן לעובד על ידי הארגון לשם צריכת תכנים לא הולמים או לא ראויים,[1] לרבות הורדה, התקנה או צפייה.
- חל איסור לגלוש ברשת ה-Darknet, לרבות שימוש בתוכנות המשמשות לאנונימיזציה, כגון דפדפן TOR.

[1] תכנים לא הולמים או לא ראויים הם: תוכן פורנוגרפי, תוכן גזעני, תוכן הכולל השמצות על רקע דת, גזע, מין, מוגבלות או מגזר, תוכן המעודד אלימות, פשיעה או טרור, הימורים, צריכת סמים וכד'.

>> שימוש מאובטח בדואר אלקטרוני

- מערכת הדואר האלקטרוני, הכתובת וכוננ הרשת הם נכסי הארגון, והשימוש בהם הוא לצורכי עבודה בלבד.
- חל איסור למסור את כתובת הדואר אלקטרוני שמקצה הארגון לעובד בעת רישום לאתרי אינטרנט שונים, למעט רישום לאתרים הקשורים לעבודה (לדוגמה, מאגרי ידע מקצועיים או הרשמה לכנסים).
- אין לשלוח מידע אישי מזהה או מידע חסוי אחר באמצעות הדואר האלקטרוני הארגוני (כולל שליחת מידע אישי באמצעות דואר אלקטרוני פנימי בין עובדי הארגון). הארגון יעמיד לרשות העובדים את הכלים הנדרשים לשם העברת מידע אישי לגורמים מורשים.
- במקרה שעובד מקבל מידע אישי רגיש באמצעות דואר אלקטרוני, עליו לשמור את המידע במקום מאובטח ברשת הארגונית ולמחוק את המידע מן הדואר האלקטרוני.
- אין לפתוח הודעות דואר אלקטרוני או קבצים המצורפים או קישורים (לינקים) ממקור לא מזוהה או חשוד. יש לדווח על כך לצוות התמיכה מיידית.

>> שימוש מאובטח במחשבים ובמערכות הארגון

- השימוש במחשבים ובמערכות הארגון האחרות יעשה לטובת העבודה בלבד. אין להשתמש בהם לצרכים פרטיים מכל סוג שהוא.
- חל איסור להשתמש במחשבים ובטלפונים הניתנים לעובד ו/או במערכות הארגון, לצורך שימושים לא חוקיים.
- כדי להימנע מהדבקה של תחנות עבודה בווירוסים או בתוכנות זדוניות, חל איסור לחבר התקנים נתיקים (Disk-on-Key, כונן חיצוני, נגני מדיה, מצלמה דיגטלית) לרשת הארגון ללא אישור של צוות התמיכה או של ממונה אבטחת המידע.

>> העברת מידע חסוי אל מחוץ לארגון

- חל איסור להוציא מידע חסוי אל מחוץ לרשת הארגונית ולמערכות המידע הארגוניות.
- העברת מידע חסוי אל מחוץ לארגון תתבצע רק לגורמים מורשים באישור ממונה אבטחת המידע, באמצעות כלים מאובטחים (כגון כספות, SFTP והצפנה). זאת כאשר העברת המידע תואמת את המטרה שלשמה נמסר המידע ובהסכמה של נושאי המידע.
- העברת מידע לגורם חיצוני תתבצע רק לאחר חתימה שלו על מסמך הצהרת סודיות (NDA).

>> אחריות העובד לשמירה על המחשבים ועל סביבת העבודה

- עובד העוזב את עמדתו ינעל את עמדת העבודה (כך שלא ניתן להפעיל את המחשב מבלי להזין שם משתמש וסיסמה), ולא ישאיר את המחשב במצב עבודה פעיל.
- באחריות העובד לוודא כי מידע חסוי אשר מודפס בעותק קשיח ואין בו צורך או שימוש ואשר אינו מועבר לתיוק, לא יושלך לפח רגיל אלא יעבור לגריסה.
- בסיום יום עבודה, על העובד להקפיד על קיום מדיניות "שולחן נקי", כלומר – כל מידע חסוי יהיה נעול במגירה או בארון.
- יש להקפיד לשמור על המחשב הנייד, אין להשאירו ללא השגחה, לרבות ברכב נעול.

>> חובת דיווח

העובד נדרש לדווח מיידית לצוות התמיכה על כל אירוע או חשד לאירוע אבטחת מידע.

להלן דוגמאות לאירועי אבטחת מידע חריגים:

- כל שינוי חריג/בלתי מוסבר באמצעי המחשוב (מישהו משתלט על המחשב ללא רשות, הופעת תוכנות או קבצים לא מוכרים, התרעות אנטי-וירוס וכו').
- קבלת הודעת דואר אלקטרוני חשודה אשר מטרתה לדלות פרטים חסויים (פישינג).
- גניבה או אובדן של מחשב נייד/טלפון חכם/רכיב מדיה נתיקה.
- חשד כלשהו כי המידע האגור במערכות נפגע (נמחק, שונה או נחשף).
- ניסיונות לדלות מידע באמצעות האינטרנט/הטלפון.
- כשל באבטחה פיזית (להודיע לקב"ט).