

**כללי אבטחת מידע והגנת הפרטיות**

מוגש מטעם יחידת אבטחת מידע והגנת הפרטיות ואגף הביטחון ברשות האוכלוסין וההגירה

סיווג: פנימי רגיש (אין להפיץ לגורמים מחוץ לרשות האוכלוסין וההגירה)

**מהי אבטחת מידע?**

***"אבטחת מידע מוגדרת ככלל האמצעים הטכנולוגיים והארגוניים הננקטים לשמירה על חסיון המידע, שלמותו וזמינותו."***

**אבטחת מידע, איך זה קשור אליי?!**

אנחנו, כעובדי הרשות, נחשפים למידע רגיש על כלל אזרחי מדינת ישראל, מבקריה, עובדים זרים ועוד אוכלוסיות שונות.

עם כניסת הטכנולוגיה לחיינו והתפתחותה, אנו רואים יותר ויותר ניסיונות לפגיעה בפרטיות המידע, גניבתו או ביצוע שימוש לרעה בו. כולנו חשופים לפגיעה כזו או אחרת!

**לכולנו היכולת לשמור ולהגן על מידע זה.**

מצמצמים את הסיכונים, מתנהגים בצורה אחראית!

*דבר המנכ"ל*

*נושא אבטחת המידע הינו בעל חשיבות גבוהה, ומחייב את כלל הרשויות במדינת ישראל להבטיח עמידה בסטנדרטים הגבוהים ביותר .עם התגברות האיומים על מערכות מבוססות מחשוב, ובכלל זה הטרור הקיברנטי, אנו נדרשים להגן על מערכות המחשוב הקריטיות של הרשות בכל הרמות, על מנת להבטיח רצף שירותי וניהולי כנדרש.*

*אני סמוך ובטוח כי כל אחד מכם יש לו את היכולת להגן על המידע שברשותו.*

*יחד – נגן על פרטיות אזרחי המדינה.*

מנכ"ל הרשות,

פרופסור שלמה מור יוסף

הכללים בחוברת זו נועדו כדי לסייע לכולנו להתנהל בצורה אחראית במרחב הסייבר, לשמור על המידע ולהגן עליו, להיות ערניים ולזהות מקרים חשודים.

יחד, נשמור ונגן על המידע שברשותנו!

# רשות האוכלוסין וההגירה מחזיקה מידע רב, חשוב ובעל ערך על תושבי מדינת ישראל, אזרחים רבים בעולם וגורמים רבים נוספים. מתוקף כך, הרשות חשופה למתקפות ואיומים שונים על המידע הרב אותו היא מחזיקה.

# יחידת אבטחת מידע מתמודדת מידי יום עם ניסיונות גורמים שונים לממש איומים אלו ולפגוע במידע הקיים ברשות.

# יחד, נוכל לזהות את האיומים על המידע

**האיומים על המידע יכולים להגיע ממספר מקורות:**

# תוצאת תמונה עבור ‪secure figure‬‏כללי

1. **תגי עובד**: יש לענוד את תג העבודה שלך על מנת שניתן יהיה לזהותך כעובד הרשות. יש להימנע מלהעביר כרטיסך לעובד אחר או להשתמש בכרטיס של עובד אחר.
2. **שיחות טלפונית**: בעת טיפול באדם שמולך, יש לוודא כי גורמים שאינם מורשים אינם נחשפים למידע רגיש.
3. **תשומת לב למתחזים**: יש לשים לב למתקשרים המבקשים מידע חריג, כגון: עובדי תמיכה המבקשים את סיסמתך, גורמים המבקשים מידע דמוגרפי מסוגים שונים על אנשים, כגון: מספר תעודת זהות או דרכון. במקרה שהתבקשת למסור מידע חריג, יש לדווח מידית ליחידת אבטחת מידע.

**זכור: נציג הרשות לעולם לא יבקש ממך את סיסמתך!**

# קבלת קהל:

1. **מבקרים/נותני שירותים:** יש לוודא כי מי שנמצא באזורי העבודה מורשה לכך. יש לשים לב לכל אדם זר/נותן שירות במקום ממודר או רגיש. אל תהססו לשאול את האדם למעשיו. במקרי הצורך, אף בקשו תעודה מזהה!
2. **פיקוח:** יש לשים לב לאורחים המסתובבים באזורים רגישים ללא פיקוח. ככל שנתקלת במקרה כזה, חובה להפנות את תשומת לב מנהל הלשכה ולפנות אל מנהל הביטחון המחוזי הרלוונטי מטעם אגף הביטחון.
3. **הפרדה בין אזורי קבלת קהל לאזורי עבודה:** וודאו כי אזורי העבודה נעולים, ולמבקרים אין גישה פנימה. הסתירו ככל האפשר מסמכים הכוללים מידע פרטי (בקשות, תעודות , אישורים וכו') בעמדות מקבלות קהל. דאגו שמסמכים הכוללים פרטים אישיים, הנמצאים על השולחן יהיו הפוכים על גבם.

# 

# ×ª××¦××ª ×ª××× × ×¢×××¨ âªoffice table cartoonâ¬âמדיניות מסך נקי

1. **הקפדה על מסך נעול:**  הקפידו על נעילת מסך המחשב בכל עזיבה של עמדת העבודה. חלה חובה לשאת את התג בכל עת.
2. **הסתרת תצוגת המסך מהקהל:** וודאו כי מסך העבודה פונה אל עמדת העבודה ומוסתר מעין הקהל.
3. **שמירה על מסך נקי:** דאגו כי על המסך לא מודבקים פתקים הכוללים סיסמאות, שמות משתמש, מספרי טלפון של עובדי הרשות וכדומה.
4. **שמירת קבצים:** יש לוודא כי לא נותרו מסמכי עבודה שלא נשמרו על מנת למנוע אובדן מידע**.** שמרו קבצים עליהם אתה עובד רק בכונני הרשת המיועדים לכך ולא על שולחן העבודה. **זכרו: מידע הנשמר על שולחן העבודה אינו מגובה ולכן לא ניתן לשחזרו בעת הצורך!**
5. **סיום העבודה:** יש לבצע התנתקות (Log off) מהעמדה בסיום יום העבודה.

**מדיניות שולחן נקי**

1. **מידע פנימי:** וודא שבסביבת העבודה לא מופיעים פרטים גלויים כמו נהלים של הרשות, דפי קשר, התכתבויות פנימיות וכד'.
2. **נגישות מסמכים במהלך העבודה:** הקפד שמסמכים רגישים לא יהיו נגישים אל הקהל, הן מבחינת צפייה והן מבחינת גישה פיזית. במקרה הצורך, נעל מסמכים אלו במגירות שולחניות או הרחק אותם מהישג יד בעת עזיבת עמדת העבודה.
3. **איסוף הדפסות מידי:** הקפד לאסוף את המסמכים שהודפסו על ידך באופן מידי על מנת שלא ייחשפו לגורם לא מורשה ואחסן אותם במקום שאושר לכך.
4. **מדפסת נקייה בתום יום העבודה:** וודא כי לא נשארו מסמכים שהודפסו על ידי עובדים אחרים במדפסת או בקרבתה בתום יום העבודה.
5. **חותמות וחומרי גלם:** במהלך היום יש לוודא כי כל חומרי הגלם והחותמות נמצאות הרחק מהישג ידם של הקהל. בסוף היום יש לדאוג לאחסן את כל החותמות במגירות או ארונות נעולים.

# ×ª××¦××ª ×ª××× × ×¢×××¨ ×××××ª ××××¢מחשוב ותקשורת

1. **ארונות תקשורת מוגנים:** במקרה שזיהית כי ארונות התקשורת אינם נעולים, כבלי תקשורת חשופים וקיימת גישה אליהם, התרע בפני מנהל הביטחון המחוזי.
2. **עבודה מהמשתמש האישי:** אל תמסור את סיסמתך לאיש, ועבוד עם פרטי המשתמש שלך בלבד.

**חל איסור חמור לחבר מכשירים ניידים או מדיה נתיקה או רכיבי מחשוב אלחוטיים (כגון: מקלדת, עכבר וכו') למחשבי הרשות!**

# 

# סיסמאות

1. **סיסמאות:** יש להימנע מלמסור את סיסמתך לכל גורם בארגון או מחוצה לו: ובכלל זאת, לנציגי תמיכה טלפוניים, לנותני שירות המגיעים ללשכה ולכל גורם הטוען כי הוסמך לכך.
2. **סיסמא חזקה:** קבעו סיסמא המורכבת מאותיות, מספרים, תווים מיוחדים – ככל שהמערכת מאפשרת זאת!
3. **לא לקבוע סיסמא חלשה:** הימנעו מקביעת סיסמא חלשה הניתנת לניחוש בקלות. אל תשתמשו בתאריכי לידה, שמות פרטיים או משפחה או כל פרט מזהה אחר בתור סיסמא. הימנעו גם מלקבוע סיסמא כרצף של אותיות או מספרים עוקבים (לדוגמא: 12345, 1111 וכדומה).

# גריסה

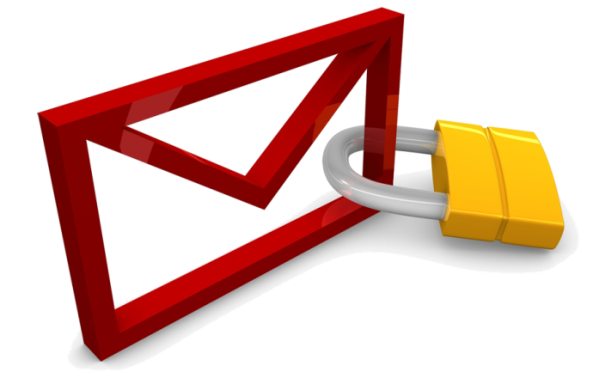
1. **אחסנת מידע לגריסה:** יש לאחסן מידע לגריסה בעמדות העבודה בתוך קרטון/ארגז אישי המסומן לכך באופן מודגש.
2. **גריסה יומית:** יש לבצע גריסה של מסמכי העבודה וחומרי הגלם הפסולים בסוף כל יום.
3. **פחי גריסה:** אין להעביר חומרי גלם שלמים או מסמכים רגישים ישירות לשק הגריסה או לחברת פינוי השקים.

# פרסומים

1. **פרסומים ברשתות חברתיות:** חל איסור לפרסם מידע פנימי או רגיש ברשתות חברתיות.

**פרסום בשם הרשות:** הרשות מנהלת את המדיה והתקשורת. חל איסור לפרסם מידע בשם הרשות, מטעם הרשות או בהמלצת הרשות ללא קבלת אישור מפורש לכך.

# דואר אלקטרוני

1. **שימוש לצרכי עבודה בלבד:** אל תירשם עם כתובת המייל הארגונית שלך לאתרים שונים כגון אתרי ביטוח ופנסיה, אתרי תשלומים למיניהם, אתרי קניות וכד'.
2. **מסירת מידע:** אל תמסור מידע רגיש באמצעות דואר אלקטרוני.
3. **שליחת מיילים:** שלח דואר אלקטרוני רק למי שמיועד לכך. אל תפיץ דואר ספאם או הודעות שרשרת. הימנע משליחת דואר אלקטרוני בתפוצות נרחבות למי שאינו מיועד לכך.
4. **קבלת מיילים:** אל תוריד קבצים או תלחץ על קישורים שהגיעו אליך באמצעות הדואר האלקטרוני מגורם שאינך מצפה לו. זהה מיילים חשודים על פי: שגיאות כתיב, בקשה לביצוע הזדהות והכנסת פרטים מזהים, הודעות המבטיחות תשלום פרסים שונים, הודעות עם תוכן מבולבל וכדומה.

**יש לדווח באופן מידי ליחידת אבטחת מידע על כל מייל חשוד שקיבלת!**

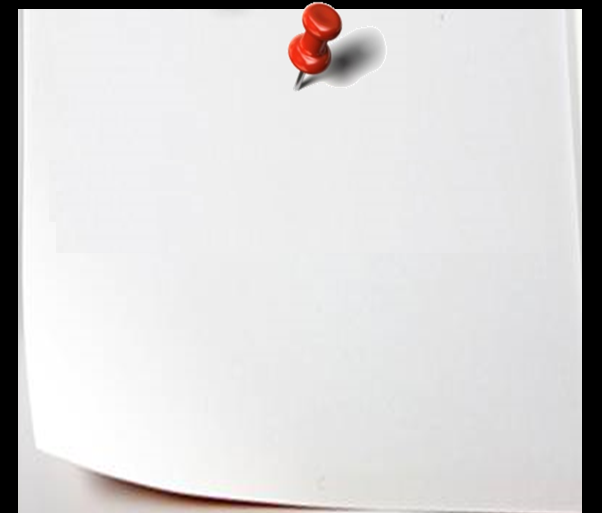
# סיום יום עבודה

1. **נעילת חדרים:** וודא כי אין קהל בחדרים הפנימיים ובשירותים, ונעל כל חדר לא מאוכלס.
2. **הפעלת מערכת האזעקה:** יש לדרוך את מערכת האזעקה ולוודא מול מוקד 99 עלהפעלתה**.**
3. **נעילת המשרד:** העובד האחרון יוודא כי החלונות סגורים והדלתות נעולות.

# הגנת הפרטיות

1. **זיהוי האזרח:**  יש לזהות את האזרח באופן דיסקרטי.
2. **הגנת הפרטיות**: אין לעשות שימוש במידע (כדוגמת שאלות זיהוי לביומטרי) שהתקבל שאינו במסגרת העבודה ובתוקף תפקידך ואחריותך.
3. **סיוע לקרובי משפחה**: חל איסור לטפל בקרובי משפחה כגון: בני/ות זוג, הורים, אחים וילדים..
4. **הגנה על האזרח**: יש להקפיד על שמירת המידע הרגיש וכבוד האזרח המוסר את המידע.
5. **הגנת הפרטיות ונגישות בעלי מוגבלויות**: **יש לתת עדיפות ולנהוג ברגישות מוגברת עם בעלי מוגבלויות.**

# הרכשה ביומטרית

1. **זכויות האזרח:** יש להסביר לאזרח טרם תהליך ההרכשה את משמעויות הפרויקט הביומטרי על מנת שהאזרח יידע את זכויותיו.
2. **הגנת הפרטיות בעת הרכשה ביומטרית**: אם מצאת כי בעל מוגבלות מרגיש שלא בנוח במעמד ההרכשה הביומטרית, יש להציע לו לבצעה במקום עם פרטיות מוגברת (כגון: עמדה אחורית או שימוש בפרגוד).
3. **מסירת מידע אמין:**  תיעוד ביומטרי ל-5 שנים משמעותו שרק תמונת הפנים נשמרת במאגר הביומטרי. תיעוד ביומטרי ל-10 שנים משמעותו כי הן טביעת האצבע והן תמונת הפנים נשמרות במאגר הביומטרי. יש להקפיד למסור לאזרחים את המידע המדויק ביותר.
4. **אפשרות הבחירה**: אפשרות הבחירה לתקופת זמן ההרכשה הביומטרית הינה נתונה לשיקול דעת האזרח בלבד. אין למסור לו ייעוץ או לכוונו לבחור באחת מהאפשרויות.

**כל אחד ממשתמשי המחשב ברשות יהיה אחראי באופן אישי לאבטחת המידע במגוון הנושאים אליהם הוא נחשף במהלך עבודתו. כל פגיעה במידע שתיגרם מרשלנות של המשתמש או מאי עמידה בנהלים תהיה באחריות המשתמש.**



נתקלת באירוע חריג?

רוצה לשאול שאלה?

יש לך הצעת ייעול?

**אנחנו זמינים!**

טלפון אגף הביטחון – 02-6294789

דוא"ל מנהל הביטחון המחוזי- נועם קרת <NoamKe@piba.gov.il>; אורי גל כפיר <OriGa@piba.gov.il>; עידן גולני <IdanGo@piba.gov.il>; יותם בלס <yotam@piba.gov.il>

טלפון יחידת אבטחת מידע – 02-6294544

דוא"ל יחידת אבטחת מידע – Infosec@piba.gov.il

עשרה כללים מנצחים לשמירה על המידע

1. **הקפדה על סיסמת משתמש מורכבת וחסויה**
2. **הקפדה על נעילת המחשב Ctrl+Alt+Del))**
3. **הימנעות מחיבור של מדיה נתיקה כמו דיסק-און-קי או טלפון סלולרי.**
4. **הימנעות מלחיצה על קישורים בדוא"ל שמקורם בגורם שאינו ידוע**
5. **הימנעות ממסירת פרטים אודות אזרחים בטלפון לגורם שאינו מורשה**
6. **הימנעות מגלישה באתרי אינטרנט לא מהימנים**
7. **הקפדה על מדיניות "שולחן נקי"**
8. **הכנסת מבקרים ונותני שירותים לאתר על פי הנוהל**
9. **שימוש במידע אליו נחשפים לצרכי עבודה בלבד- אין לחשוף מידע לגורמים שאינם מורשים**
10. **דיווח ללא דיחוי על כל אירוע אבטחת מידע למנהל הביטחון המחוזי ולמנהל אבטחת מידע**