מועצה אזורית הגלבוע
לשכת ראש המועצה

# נוהל אבטחת מידע

## כארגון יש לנו מידע חשוב ורגיש ויש לנו אחריות רבה בהגנה עליו.

אבטחת מידע

נתקלנו בשנה האחרונה בפירסומים על לא מעט מקרים בהם אירגונים לא בחלו באמצעים כדי להוציא מידע על פעילות הארגון או על תושבים ו/או ספקים ו/או עובדים.

צריך לקחת בחשבון, שהתפקיד שלנו, כעובדי הארגון, הוא לשמור על נאמנות למועצה ולתושבים ולעשות כל האפשר שמידע לא ידלוף מהחברה החוצה..

.התפקיד שלנו, כעובדי הארגון, הוא לשמור על נאמנות למועצה ולפעילותה, ולעשות כל האפשר שמידע רגיש לא ידלוף מהמועצה החוצה.

להלן כמה **נהלי אבטחת מידע** שיעזרו לנו לשמור על המידע הארגוני.

## הוצאת מידע החוצה

מיותר לציין שהעובדים מחויבים לסודיות כלפי החברה, וברור שאין להעביר מידע, לצלם או לשלוח לאף גורם חיצוני כל מידע רגיש, אלא במסגרת העבודה ולאנשים הרלוונטיים שמוסמכים לכך. אי ציות לנוהל זה מהווה הפרה בסיסית של חובת העובד לאירגון ויהווה עילה לפיטורין ובמקביל ישמש בסיס לתביעה משפטית. ."

## חובת הסודיות

חובת הסודיות היא חובה בסיסית ואינה מוגבלת בזמן. גם עובד שהתפטר או פוטר עדיין נשאר על פי החוק וההסכמים מחויב לסודיות בכל מה שקשור למידע הרלוונטי לאירגון, אליו נחשף במהלך התקופה בה עבד בחברה.

## מסמכים רגישים/ גריסה

אין להשאיר מסמכים רגישים במקום גלוי וחלה חובה לשמירת מידע רגיש באופן בטוח..

אסור להשליך לאשפה מסמך עם רגישות כל שהיא. יש לגרוס כל מסמך, שרטוט, טיוטה או פקס עם מידע רגיש, שלא נחוץ יותר.

WWW.hagilboa.org.il e-mail: oved@hagilboa.org.il
מועצה איזורית הגלבוע , ד.נ. גלבוע 18120 מוקד אזורי 109 , טל. 6533200 - 04 , פקס. 6531451 - 04

מועצה אזורית הגלבוע
לשכת ראש המועצה

## רלוונטיות המידע

כל עובד עשוי להיחשף למידע הרלוונטי לעבודתו בלבד. אין לקרוא, לפתוח, להעתיק או לצלם חומר שלא בסמכות או לא רלוונטי לעבודת העובד, בלא אישור לכך מהגורם הרלוונטי באירגון- כמנהל אגף או מנכל.

## אורחים ומבקרים

כל אורח/מבקר יוכנס אל המשרדים רק לאחר וידוא מול הגורם שהזמין אותו שאכן הוא מוזמן ורשאי להיכנס. יש להקפיד שלא יחשף מידע רגיש בפני אורחים ומבקרים..

## מיקום הפגישות

יש לקיים פגישות עם אורחים בחדר ישיבות.
בחדרי העבודה יש מסמכים ומסכי מחשב גלויים שעלולים להיחשף.

## השימוש בסלולרי

אין לצלם מסכי מחשב או מסמכים רגישים שלא לצרכי עבודה. במידה ויש צורך לצלם כחלק מתהליך העבודה, יש לדאוג להעביר את התמונה למחשב ולמחוק אותה מיד לאחר השימוש בה.

## דואר אלקטרוני

משלוח מסמכים ללקוחות, ספקים, אנשי מקצוע וכו', יבוצע באמצעות המייל של המועצה בלבד. זה חשוב גם משיקולים אירגוניים וגם משיקולי אבטחה..

## מסמכים רגישים

העברת מסמכים רגישים, (כגון מידע על תושבים, עובדים, תכניות חשובות, מסמכים המכילים מידע כלכלי רגיש וכו') תתבצע במסמך מוצפן. את הסיסמא לפתיחת המסמך יש להעביר במדיה אחרת כגון טלפון סמס או וואטסאפ. כך נוכל להגן על המסמך מפני מי שלא אמור לקרוא אותו. יש להשמיד את המסמכים בתום הקריאה..

## דואר חיצוני

יש להשתמש לצרכי העבודה אך ורק במייל של החברה, אין להעביר מידע של החברה דרך שירות דואר אחר כגון ,GMAIL וואללה, הוט מייל וכו.'

## אחסון חיצוני

אין לשמור חומר השייך לעבודה על דיסק חיצוני

## חיבורים לUSB-

מאחר ויש אפשרות לחבר מכשירים רבים ושונים לשקע ה USB-מצלמות, סלולריים, דיסק און קי וכו'), מהווה יציאה זו מהמחשב פרצת אבטחה..

מועצה אזורית הגלבוע
לשכת ראש המועצה

## סיסמאות

כל עובד צריך להיחשף רק לסיסמאות הנחוצות לו לצורך העבודה (סיסמא למייל, למחשב, לתוכנות, למסמכים וכו'), אין לבקש סיסמאות מעובד אחר ואין להעביר בלי אישור סיסמאות למי שלא מחויב להיחשף להן לצרכי עבודה.

## סיבוכיות הסיסמאות

אין להשתמש בסיסמאות פשוטות כגון 1234 או 12345 וכו'. זמן הפיצוח שלהן נמדד בשניות.
כדאי לבחור סיסמא עם משמעות אישית וכאלה המורכבות מאותיות ומספרים.

## שמירת סיסמאות

אין לרשום סיסמאות על פתקים או דפים ולהניחם בסמוך למחשב. המקום לשמירת סיסמאות הוא במסמך מוצפן עם סיסמא מורכבת.

## מחשבים ניידים

מחשב נייד הוא מוצר שיכול להיגנב. לכן, אין לשמור מידע רגיש על מחשב נייד. יש לשמור את כל המידע על השרת. בצורה זו, אבדן המחשב הנייד לא יהפוך לבעיית אבטחה. אין להחזיק מידע ששייך לעבודה על מחשב פרטי של עובד, ללא אישור.

## התקנת תוכנות

אין להתקין על מחשבי החברה תוכנות ממקור חיצוני ללא אישור. תוכנות "חינמיות" חיצוניות, עלולות להכיל רכיבים שהנזק שלהן למערכת רב.

## השארת חומר ברכב

רכב אפשר לפרוץ או לגנוב ולכן אין להשאיר חומר רגיש ברכב ללא השגחה.

## מייל ממקור זר

אין לפתוח מייל שהגיע ממקור לא ידוע ובוודאי שלא להיכנס לקישור, שמופיע במייל, אם לא ברור לנו מה המקור ומבלי שידוע לנו שהוא אמין ולגיטימי. מייל כזה יכול לגרום לנזק רב למסמכי הארגון או לחשוף אותו לריגול תעשייתי.

## אתרים מפוקפקים

יש להמנע מכניסה לאתרים לא מוכרים. כניסה לאתרים כאלה, עלולה להעביר וירוס הרה אסון אל המחשב שלך ועלולים לגרום לנזק רב למחשב ו/או למערכת כולה.
בנוסף, אתר כזה עלול לבצע הצפנה לכל קבצי המידע ברשת ולדרוש כופר של אלפי דולרים כדי לקבל את המידע בחזרה. לכן יש להיזהר מאוד מכניסה לאתרים מהסוגים האלה.

**ככלל, בכל הנוגע לאבטחת מידע,**
**ככל שיש ספק- אין ספק. יש לפנות אל הממונה על מערכות המידע ולבקש את אישורו.**