

נוהל אבטחת מידע



1



תוכן

4	כללי	1.
4	מבוא	1.1
4	סיכונים	1.2
4	מטרות	1.3
5	תכולה ותוקף	1.4
5	סימוכין	1.5
5	הגדרות	1.6
6	הפרדת סמכויות	1.7
6	אחריות	1.8
7	סקרי סיכונים	1.9
7	ניהול שינויים	1.10
7	ניהול אירועי אבטחת מידע	1.11
8	הגורם האנושי	2.
8	קבלת עובד	2.1
9	עזיבת עובד	2.2
9	אבטחה לוגית	3.
9	עבודה שוטפת בשרת קבצים	3.1
9	עבודה שוטפת במערכת ליבה	3.2
9	ניהול ובקרה	3.3
10	הקשחת תחנות עבודה	3.4
10	אבטחה פיזית	4.
10	מחשבים ניידים	4.1
11	מכשירים ניידים	4.2
11	ציוד ואחסון נתונים	4.3
11	תיעוד תשתיות ונכסי מחשב	4.4
11	כניסה לחדר שרתים	4.5
12	ציוד אבטחה	4.6
12	גיבוי/שחזור והתאוששות	5.
12	גיבוי	5.1



12.....	שחזור	5.2
13.....	אבטחת תקשורת ואינטרנט	6.
13.....	תעבורת מידע	6.1
13.....	התחברות מרחוק	6.2
13.....	מודעות העובדים	6.3
14.....	אינטרנט אלחוטי	6.4



1. כללי

1.1 מבוא

עובדי רשויות מקומיות עושים שימוש במערכות המידע השונות במהלך עבודתם. מערכות המידע מכילות נתונים רבים על הארגון בכל תחומי פעילותו. נוהל זה נועד להבטיח כי ננקטים הליכים מספקים לאבטחת המידע.

אבטחת המידע נועדה למנוע ככל הניתן פגיעה במאגרי המידע ובמערכות התקשוב של הארגון, ולצמצם בכך את סיכוני הפגיעה בתפעולו הסדיר. בנוסף, מטרת נוהל זה אלו להעלות את המודעות והאחריות האישית של עובדי הרשויות לנושא האבטחה. דרישות אבטחת המידע ייקבעו על פי החוקים והתקנים בנושא.

רשויות מקומיות מחויבות לעמוד בחוק ותקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, שפורסם ע"י משרד המשפטים ונכנס לתוקף במאי 2018.

1.2 סיכונים

סיכונים אליהם חשוף הארגון:

- א. שימוש לרעה במידע רגיש המצוי במאגרי המידע של הרשות, ע"י חשיפת פרטים אישיים של תושבים, חברות, מפעלים וחומרים מקצועיים רבים.
- ב. גרימת נזק תדמיתי וכלכלי בלתי הפיך, כתוצאה מהשבתת מערכות מחשוב, גרימת זמן השבתת פעילות וחוסר מענה לתושבים, לחברות ומפעלים.
- ג. שיבושים בפעילות השוטפת של הארגון בעזרת שינוי, מחיקה או העברה לצד שלישי של המידע הארגוני.
- ד. השבתת פעילות ביטחונית במצבי חירום, ע"י שיבוש או ניתוק תשתיות תקשורת.

1.3 מטרות

- מטרת נוהל זה היא להגדיר הוראות לשימוש ותפעול נאות במשאבי המחשוב של הארגון, על ידי העובדים, משלב התחלת העבודה ועד עזיבת העובד. הנוהל מגדיר את הנושאים הבאים:
- א. מתן הרשאות לעובד בתחילת עבודתו (הן בשרת הקבצים והן במערכות ליבה ממוחשבות).
 - ב. שמירה על מידע במהלך העבודה.
 - ג. טיפול בהרשאות בעזיבת עובד.
 - ד. הנחיות לשימוש שוטף במשאבי המחשוב של הארגון.

1.4 תכולה ותוקף

- 1.4.1 נוהל זה חל על כל העובדים של הרשויות המקומיות, המשתמשים במערכות מידע הפנים ארגוניות או במערכות חיצוניות המשרתות את הרשויות.
- 1.4.2 לאחר החלטת הארגון על אימוץ הנוהל המוצע ע"י אשכול גליל מערבי, הנוהל:
- 1.4.2.1 יאושר ע"י מנכ"ל/מזכיר הרשות
 - 1.4.2.2 יצורף לספר נהלים של הארגון
 - 1.4.2.3 ינוהל במהדורה עצמאית
 - 1.4.2.4 יהיה תקף מיום פרסומו

1.5 סימוכין

קובץ התקנות-7809 / ת"י 27000 / ISO 27001

1.6 הגדרות

- 1.6.1 מידע – נתונים, סימנים, מושגים או הוראות למעט תוכנה, המאוחסנים במחשב או אמצעי אחסון אחר (דיסק חיצוני, דיסק נייד וכדומה).
- 1.6.2 אבטחת מידע – שמירת חיסיון, זמינות, שלמות ושרידות של מידע בארגון.
- 1.6.3 אירוע אבטחת מידע – כל מקרה בו קיים חשד לפגיעה בסודיות, אמינות או זמינות במערכות הארגון, המידע הארגוני או כל אמצעי אחר אשר שייך למערכות המידע הארגוניות. פגיעה בשלמות המידע, שימוש במידע ללא הרשאה או חריגה מהרשאה.
- 1.6.4 אירוע אבטחה חמור – הוא אירוע בו נעשה שימוש במידע ממאגר המידע שחלה עליו רמת אבטחה גבוהה, בלא הרשאה או בחריגה מהרשאה או שנעשתה פגיעה בשלמות המידע.
- 1.6.5 חיסיון – הבטחת נגישותו של מידע רק לגורמים מורשים.
- 1.6.6 זמינות – הבטחה שמשמשים מורשים יוכלו לגשת למידע ולמשאבים לפי הצורך והגדרה מראש.
- 1.6.7 משתמש – כל מי שמשמש במשאבי המחשב של הארגון.
- 1.6.8 שרת – מחשב המאפשר פעילות משותפת לכלל המשתתפים.
- 1.6.9 מערכות ליבה – מערכות ממוחשבות לניהול פעילות מידע ארגוני.
- 1.6.10 מערכת אורחת – מערכת ממוחשבת אשר מתחברת לתשתית התקשוב של הארגון ואינה באחריותו.
- 1.6.11 ממונה אבטחת מידע – בעל תפקיד בארגון אשר אחראי על רגולציה ותקינות אבטחת המידע בארגון.
- 1.6.12 מנמ"ר (מנהל מערכות מידע) – האדם האחראי על בניית אסטרטגיית המחשוב ועל תכנון, ניהול ובקרה של מערכות מידע בארגון.
- 1.6.13 מנהל מחשוב – האדם האחראי על תפעול של כל הפתרונות הטכנולוגיים בתחום המחשוב בארגון (אופק חדש).



1.6.14 סקר סיכוני אבטחת המידע – תהליך אשר מאפשר לקבל תמונת מצב עדכנית המשקפת את מצב אבטחת המידע בתשתיות המחשוב של הארגון.

1.7 הפרדת סמכויות

- 1.7.1 ברשויות מקומיות קיימות מספר סוגים של מערכות מידע:
- 1.7.1.1 מערכות AD ו-DC לניהול משתמשים וישויות בארגון.
 - 1.7.1.2 מערכות לשמירת קבצים (FILE SERVER).
 - 1.7.1.3 מערכות ליבה (פתרונות תוכנה של חברות - מטרופולינט, אוטומציה החדשה, EPR ועוד).
 - 1.7.1.4 מערכות דואר (EXCHANGE או OFFICE 365).
 - 1.7.1.5 מערכות שרתי טרמינל לחיבור מרחוק. המערכות מותקנות על גבי שרתים שונים.
- 1.7.2 מערכות ליבה, בכל אחת מהרשויות, מנוהלות ע"י ספקי הפתרונות. הספקים אחראיים באופן בלעדי על תמיכה ושירות במערכת, על המודולים השונים שלהן, כולל על מערכת ההרשאות, ואבטחת המידע (בהתאם לחוקים והתקנות העדכניות בנושא זה).
- 1.7.3 מערכות פנים ארגוניות לניהול הידע הארגוני, ניהול הקבצים והדוא"ל וכן כל התשתיות מנוהלות ע"י צוות IT של אשכול גליל מערבי, כולל נוהל משתמשים והרשאות. המנמ"ר אחראי ליישום כלל הנהלים הנוגעים למערכות מידע השונות.

6

1.8 אחריות

- 1.8.1 כל משתמש אחראי באופן אישי לכלל המידע המצוי בחזקתו, לרבות כזה אשר נשלח או הועבר אליו. כמו כן, האחריות לקיום הנחיות ומדיניות אבטחת המידע של הארגון מוטלת על כל משתמש ומשתמש ברשות המקומית. כל עובד אחראי לנעילת המחשב ולשימוש בסיסמה.
- 1.8.2 מנהלים יישאו באחריות כוללת ליישום נהלי אבטחת המידע בתחומי סמכותם לפעילות עובדיהם מהיבטי אבטחת המידע.
- 1.8.3 לפי תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, תקנה (א19), חוק הגנת הפרטיות מטיל אחריות אישית על אבטחת המידע במאגר על בעל המאגר, המנהל והמחזיק.
- 1.8.4 בעל מאגר מידע יגדיר במסמך הגדרות מאגר, את כל העניינים הדרושים לפי תקנות הגנת הפרטיות, תקנה (א2).
- 1.8.5 מנהל משאבי אנוש אחראי לוודא, כחלק מעזיבת עובד, שטופס העזיבה נחתם על ידי מנהל מחשב.
- 1.8.6 נהלי אבטחת המידע של הרשות המקומית חלים על כל עובדי הארגון וכל אדם אחר, הפועל עבור הרשות.
- 1.8.7 הרשות המקומית תמנה אדם מהארגון לתפקיד ממונה אבטחת מידע, אשר יהיה אחראי על זיהוי, ניטור, ניתוח ופיקוח פעולות הארגון ויישום רגולציה במטרה להגביר את רמת אבטחת המידע בארגון. הממונה יתכנן הדרכות תקופתיות בנושא הגברת מודעות אבטחת מידע וכן יעביר תזכורות ועדכונים שוטפים בנושא לכלל עובדי הארגון. הפעילות תבוצע בהתאם לתכנית עבודה שתאושר ע"י המנכ"ל בתחילת כל שנה.



- 1.8.8 הרשות המקומית תעגן בחוזה החלת נהלי אבטחת מידע על כלל המשתמשים החיצוניים, ועל כל יתר הגורמים אשר יש להם מעורבות בפיתוח, בתפעול ובתחזוקה של מערכי המידע, השליטה והבקרה, כולל יועצים וספקי "מיקור-החוץ" ("OUTSOURCING").
- 1.8.9 הרשות המקומית תפעל על פי נהלים והנחיות של רשות הסיבר כפי שיפורסמו ויעודכנו מעת לעת.
- 1.8.10 פגיעה בזדון במידע, או במערכות מחשוב של הארגון, או ניסיון לכך, מהווה עבירה פלילית, על חוק המחשבים התשנ"ו – 1996.
- 1.8.11 כל חריגה מהוראות נוהל זה, תתאפשר אך ורק לאחר פניה מנומקת בכתב ואישור בחתימה של מנכ"ל הרשות המקומית, ושל ממונה אבטחת מידע. כל המסמכים הללו יתויקו וישמרו בתיק מיוחד במחלקת משאבי אנוש, וכן בתיק אבטחת מידע ארגוני תחת בקשות לחריגה.

1.9 סקרי סיכונים

- 1.9.1 כל רשות מקומית תבצע סקר סיכוני אבטחת מידע ומבדקי חדירה תקופתיים על ידי גורם חיצוני. פרק הזמן בין הסקרים לא יעלה על 24 חודשים. ממצאי הסקר יועברו להנהלת הרשות ועל פיהם ייקבעו הבקורות וההתליכים להקטנת הסיכונים.
- 1.9.2 ממונה אבטחת מידע ייזום בדיקות פנימיות לגילוי כשלי אבטחת מידע במערכות המידע של הרשויות ויפעל לתיקון הליקויים במידה ויתגלו. הבדיקות יבוצעו בהתאם לתכנית עבודה שתאושר ע"י המנכ"ל בתחילת כל שנה.

1.10 ניהול שינויים

איסור שינוי לא מבוקר - חל איסור על ביצוע שינוי בנתונים, בתוכנות יישומיות, הגדרות תשתית מחשוב ובחומרה, אלא אם הדבר נעשה באופן מאובטח, מבוקר ומתועד ובהתאם להנחיה מפורשת ובקרה של המנמ"ר. כל שינוי שיבוצע, יתועד ויתויק בתיק אבטחת מידע רשותי תחת ניהול שינויים.

1.11 ניהול אירועי אבטחת מידע

- 1.11.1 אירועי אבטחת המידע המאותרים על-ידי עובדי הארגון, ידווחו לממונה אבטחת מידע ברשות והנ"ל ידווח למנמ"ר באימייל לכתובת cio@wegalil.org.il ויועברו על ידו לפי הצורך להמשך טיפול וחקירה ע"י בעלי מקצוע מוסמכים. מסקנות התחקיר יועברו למנכ"ל וממונה אבטחת מידע של הרשות המקומית.
- 1.11.2 מחובתה של הרשות המקומית לתעד אירועי אבטחת מידע שהתרחשו, כדי לייצר היסטוריית אירועים חריגים ולהפיק מהם לקח לעתיד. אירועי אבטחה יתועדו ויתויקו בתיק אבטחת מידע תחת אירועי אבטחה.
- 1.11.3 ממונה אבטחת מידע יתאם ישיבות קבע תקופתיות עם מנכ"ל וקב"ט הרשות והמנמ"ר, לצורך דיון בנושא אירועי אבטחת מידע - ניתוח האירועים ועדכון תכנית התמודדות עמם.



נוהל התמודדות עם אירועי אבטחת מידע הארגוני ינוהל לפי מהדורה עצמאית ומתעדכן באופן נפרד מנוהל אבטחת מידע, בפרקי זמן שונים, לפי הצורך והשינויים במבנה מערך הגיבוי הארגוני.

2. הגורם האנושי

2.1 קבלת עובד

- 2.1.1 כל עובד המתקבל לרשות מקומית יקבל הדרכה ע"י ממונה אבטחת מידע, בכל הנוגע בשימוש נכון במערכת המחשב ועל אופן השמירה והגנה על מידע. על העובד לחתום על טופס קבלת תנאים כתנאי לקבלת משתמש והרשאה.
- 2.1.2 מנהל מחלקה של העובד החדש ימלא טופס בו יציין את פתרונות המחשוב, בהן ישתמש העובד במסגרת תפקידו:
- 2.1.1.1 מערכת ליבה ומאיזה סוג.
 - 2.1.1.2 מערכת לניהול הידע הארגוני ואיזה סוג.
 - 2.1.1.3 תוכנת אופיס.
 - 2.1.1.4 תיבת דוא"ל הארגוני.
 - 2.1.1.5 מאחסן קבצים בשרת הארגוני.
 - 2.1.1.6 מתחבר מרחוק למערכות הרשות.
- 2.1.2 במערכות ליבה יינתנו הרשאות על פי תפקיד העובד. לגבי כל עובד, יקבע מנהל המחלקה את ההרשאות שיש לתת לעובד עם תחילת עבודתו. מנהל מחלקה יעביר למנהל מחשוב של הרשות הרשאות נדרשות לעובד.
- 2.1.3 לכל עובד תפתח ספרייה בשרת הקבצים השייכת אליו בלבד. בתפן תיקיית Z:
- 2.1.4 כל משתמש יקבל סיסמה ראשונית כתנאי להתחלת עבודתו במערכת. הגדרת הסיסמה מורכבת ממינימום 7 תווים כולל אותיות קטנות/גדולות ומספרים.
- 2.1.5 הסיסמה הראשונית תשמש לצורך כניסה ראשונית חד-פעמית למערכת. עם כניסתו הראשונה לחשבונו במערכת, על המשתמש להחליפה לפני כל פעולה אחרת. מכאן והלאה הסיסמה תוחלף ע"י המשתמש ובאחריותו.
- 2.1.6 כל עובד ינהל עד שלושה חשבונות משתמש שונים וסיסמאות אליהם – לרשת מחשוב של הארגון ו/או למערכת ליבה ו/או למערכת התחברות מרחוק (VPN Client).
- 2.1.7 חל איסור מוחלט למסור/לחשוף סיסמאות. אין לתלות את הסיסמאות על פתקיות בקרבת המחשב.
- 2.1.8 ככלל, תוחלפנה סיסמאות אחת לשישה חודשים. המערכת תכפה את החלפת הסיסמה על המשתמש. המשתמש יקבל התראה על מסך המחשב על סיום תוקף הסיסמה לפחות 7 ימים טרם פקיעתה. אין לחזור על סיסמאות קודמות במשך 10 "הדורות" האחרונים.
- 2.1.9 במקרה של הקלדת סיסמה שגויה, תחסם התקשורת ותוצג על כך הודעה במסך. המערכת תאפשר חמישה ניסיונות כניסה, לאחר מכן תחסם התקשורת לחלוטין. חידוש הגישה של המשתמש אל



המערכת יתאפשר רק אחרי קיומו של בירור ובקשת חידוש באמצעות מנהל היישוב. במקרה הצורך יועבר המקרה לידיעת הממונים הרלוונטיים.

2.2 עזיבת עובד

- 2.2.1 כל עובד שעוזב ולו הרשאות גישה למערכת יקבל, כחלק מהליך עזיבתו, אישור החתום על ידי מנהל מחשוב של הרשות, אשר ידאג להחלפת הסיסמה או להגדרת העובד כ – DISABLED לפי הצורך. במערכות ליבה יוגדר העובד כלא פעיל.
- 2.2.2 אחת לרבעון תתבצע פעילות ביטול או הקפאת משתמשים שלא עשו שימוש במשאבי המחשוב, במשך תקופה שתוגדר בזמן הבדיקה. על מנהל משאבי אנוש או מי שנקבע ע"י הרשות לעדכן מיד למנהל מחשוב על עזיבת כל עובד.

3. אבטחה לוגית

3.1 עבודה שוטפת בשרת קבצים

- 3.1.1 כל עובד ישמור את הקבצים השונים על גבי הרשת, במחיצות היחידתיות והאישיות שהוקצו לכל משתמש בשרת, שיהיו תלויות בהרשאות כניסה. כאשר מספר משתמשים עושים שימוש במידע באותה מחיצה, יגדיר מנהל מחשוב מחיצה משותפת.
- 3.1.2 לאחר פרק זמן של 30 דקי שעובד לא פעיל בתחנת העבודה, התחנה תינעל באופן אוטומטי.
- 3.1.3 אין לאפשר גישה למחשבים האישיים או לחשוף המידע המאוחסן במחשב, בפני עובדים אשר אין המידע נחוץ להם לצורך עבודתם וכן בפני גורמים שאינם עובדי הרשויות, באשר הם.

3.2 עבודה שוטפת במערכת ליבה

- 3.2.1 לכל עובד תוגדר סיסמה למערכת בהתאם לנדרש בסעיף (2.1.4) בנוהל זה.
- 3.2.2 מנהל מחלקה יגדיר לכל עובד הרשאות נדרשות במערכת ליבה הארגונית.

3.3 ניהול ובקרה

- 3.3.1 המנמ"ר יקבל מידע ממונה אבטחת מידע על ניסיונות כניסה לא מורשים למערכת. ויבדוק מידע זה, לאיתור ניסיונות פריצה של לא מורשים.
- 3.3.2 לאחר 10 ניסיונות כניסה כושלים של אנשי מחשוב, תחסם הכניסה למערכת ממנה בוצעו הניסיונות הכושלים. אפשרות לכניסה מחודשת תינתן לעובד על ידי מנהל המערכת.
- 3.3.3 ממונה אבטחת מידע ידאג שספק פתרון של מערכות ליבה יוציא אחת למספר חודשים רשימה של כל המורשים להיכנס ויודא:
- 3.3.3.1 שכל העובדים שעזבו הוגדרו כ-"לא פעילים".
- 3.3.3.2 שלכל משתמש שהוגדרו לו הרשאות למערכת, עושה שימוש בסיסמה.



3.3.3.3 שההרשאות מתאימות לתפקידים של אותם העובדים.

3.3.4 חל איסור מוחלט על הבאת תוכנות זרות לשימוש במחשבי הארגון שלא אושרו ע"י מנהל מחשב.

3.3.5 על המשתמש לוודא הימצאות תוכנת אנטי-וירוס פעילה במחשבים האישיים ואין להפסיק את פעולתה.

3.4 הקשחת תחנות עבודה

3.4.1 הקשחת תחנה תבצע באמצעות הפעלת מדיניות קבוצתית ב-Active Directory.

3.4.2 משתמשים בתחנות עבודה לא יוגדרו כ-Administrator.

3.4.3 לכל מחשב של משתמש תהיה הרשאה אחת לשימוש בדיסק און ארגוני. המעקב אחר מספרי דיסק און כי ולאילו מחשבים יש להם הרשאה יבוצע ע"י טבלה ייעודית שתנוהל ע"י ממונה מערכות מידע.

3.4.4 במידה ויש למשתמש צורך במתן הרשאה לגישה/חיבור של התקן מכל סוג שהוא למחשב הארגוני, המשתמש יגיש בקשה בנושא הכוללת את נימוק הצורך לממונה אבטחת מידע. הנ"ל ידאג להעביר בקשה זו למנמר ובהתאם למנהל המחשב. כל בקשה כזו תתועד בתיק אבטחת מידע תחת בקשה לגישה של התקן למחשב.

3.4.5 ברשות יהיה מוגדר מחשב אחד (לדוגמא מחשב של חדר ישיבות) שאינו מוקשח ואליו תהיה גישה להתקנים חיצוניים. במחשב זה לא תהיה הרשאת גישה לרשת המשותפת מלבד תיקייה ייעודית. ברשת תיפתח תיקייה ייעודית תחת שם "חדר ישיבות", ולה גישה לכל עובדי הארגון.

10

4. אבטחה פיזית

4.1 מחשבים ניידים

4.1.1 חיבור מחשב נייד לרשת תקשורת של הארגון יתבצע רק לאחר שמנהל מחשב יודא קיום של אמצעי הגנה הולמים במחשב וברשת הארגון.

4.1.2 חל איסור לאגור נתונים על גבי דיסק קשיח במחשב נייד, אלא אם כן מותקן במחשב אמצעי בקרה ואבטחה המאושרים ע"י מנהל מחשב.

4.1.3 אין להשאיר מחשב נייד ברכב ללא השגחה אישית וישירה של בעל המחשב הנייד. אם נגב מחשב נייד או שיש חשש כי המידע האגור בו נחשף בפני גורם זר, יש לדווח מיידית לממונה אבטחת מידע, הנ"ל ידווח לקב"ט הרשות ולמנהל מחשב.

4.1.4 אין להשאיר מחשב נייד ללא השגחה במשרד/חדר ישיבות לא נעולים.

4.1.5 מחשב נייד יהיה מוגן בסיסמאות בהתאם להנחיות בסעיף 2.1.6 של נוהל זה.

4.1.6 ממונה אבטחת מידע ינהל טבלת מעקב אחר המחשבים הניידים הקיימים ברשות, ואצל מי הם נמצאים.



4.2 מכשירים ניידים

- 4.2.1 בכל מכשיר נייד (סמרטפונים וטאבלטים) אשר מחוברים לרשת תקשורת של הארגון יותקן אנטי-וירוס.
- 4.2.2 כל מכשיר נייד יקבל הרשאות כניסה לרשת תקשורת של הארגון לפי צרכי שימוש ובאישור מנהל רשת בלבד.
- 4.2.3 בתשתיות תקשורת האלחוטיות של הארגון תוקם רשת נפרדת לטובת אורחים המבקרים, המאפשרת יציאה לענן האינטרנט בלבד.
- 4.2.4 במקרה של אובדן מכשיר נייד, יש להודיע לממונה אבטחת מידע, והנ"ל ידווח למנהל מחשוב באופן מיידי.
- 4.2.5 בכל מכשיר נייד תוגדר תצורת אבטחה אחידה (סיסמה, טביעת אצבע, דפוס וכדומה).

4.3 ציוד ואחסון נתונים

- 4.3.1 אין לחבר התקנים חיצוניים לא מוכרים (USB, Disk-On-Key, טלפון סלולארי) למחשב ללא קבלת אישור ממנהל מחשוב, וזאת בהתאם לסעיף 3.4.4.
- 4.3.2 תותקן ותנוהל באופן שוטף מערכת בקרה אשר תגביל שימוש במדיה חיצונית הלא מאושרת.
- 4.3.3 התקן חיצוני אשר יאושר לשימוש ברשת הארגונית יהיה מוצפן, לשימוש העובד שקיבל את ההתקן בלבד ובאחריותו האישית לא להעביר את ההתקן לגורם אחר.

4.4 תיעוד תשתיות ונכסי מחשב

- 4.4.1 מנהל המחשוב/מנמ"ר ינהל תיעוד מלא של יחסי גומלין בין "חומת האש" (Firewall) לציוד תקשורת הארגוני (כגון נתבי תקשורת, שרתים וציוד אחסון חיצוני).
- 4.4.2 מנהל המחשוב/מנמ"ר ינהל תיעוד מלא של מחשבים נייחים וניידים, כולל רשימת תוכנות מותקנות והיררכיית הרשאות ברשת הארגונית.
- 4.4.3 מנהל המחשוב/מנמ"ר יעביר לממונה אבטחת מידע אחת לחציון/שנה דוח תיעוד בהתאם לסעיפים 4.4.1 ו 4.4.2

4.5 כניסה לחדר שרתים

- 4.5.1 הכניסה לחדר שרתים תתאפשר לגורמים מורשים בלבד או בליווי שלהם.
- 4.5.2 רשימת הגורמים המורשים לכניסה לחדר שרתים תוקם ותנוהל ע"י מנהל מחשוב ותועבר למנכ"ל הרשות המקומית לאחר כל שינוי/עדכון.
- 4.5.3 מפתח מחדר שרתים נמצא אצל שני אנשים בלבד שנקבעו מראש ע"י מנכ"ל הרשות המקומית.

4.6 ציוד אבטחה

- 4.6.1 הארגון ירכוש, יתחזק וישדרג מערכת "חומת אש" (Firewall) לאבטחת וסינון התעבורה אל ומהרשת העסקית אל רשת האינטרנט, כולל תעבורה מוצפנת (SSL).
- 4.6.2 תותקן ותתחזק מערכת Mail Relay, המאפשרת סינון ומניעה של "דואר זבל" או כזה החשוד כמכיל פוגען העלול לפגוע ברשת הארגון. הסינון נדרש להיות דו-סטרי.
- 4.6.3 מתגי תקשורת נדרשים להיות מנוהלים, מנוטרים ומוקשחים לפחות ברמת כתובות חומרה של ציוד המחשוב (MAC Address).

5. גיבוי/שחזור והתאוששות

5.1 גיבוי

- 5.1.1 גיבוי של כל סוגי המידע הארגוני יתבצע בצורה אוטומטית בתדירות ובזמנים קבועים מראש. נוהל גיבוי יקבע בין מנהל המחשוב/מנמ"ר מול הרשות. הנוהל יתויק בתיק אבטחת מידע תחת "גיבוי".
- 5.1.2 פתרון הגיבוי יכלול לפחות סוג אחד של גיבוי מקומי (מאוחסן במבנה הרשות המקומית) ולפחות סוג אחד של גיבוי בענן (הוצאת נתונים מחוץ למבנה הרשות).
- 5.1.3 ציוד של אחסון גיבויים במבנה הארגון וגישה לגיבוי בענן יהיו מוגנים ע"י כניסה מאובטחת ומבוקרת.
- 5.1.4 כל פתרונות הגיבוי יספקו דיווח מפורט על תקינות תהליך הגיבוי בסימום, ע"י משלוח הודעה ב-email והפקת קובץ LOG. ממונה המחשוב יעביר דוח תקינות כל חציון לממונה אבטחת המידע.

5.2 שחזור

- 5.2.1 שחזור ראשוני של המידע מתוך גיבוי יתבצע אל "עמדת בדיקה ייעודית" - מחשב עצמאי לא מחובר לרשת הארגון. המידע יועבר למחשבי המשתמשים רק ע"י מנהל מחשוב ובתיאום עם ממונה אבטחת מידע וזאת לאחר בדיקת תקינות ו-"ניקיון החומר".
- 5.2.2 שחזור המידע מהגיבוי יתבצע אך ורק ע"י מנהל מחשוב של הרשות המקומית או בנוכחותו ובנוכחות ממונה אבטחת מידע.

נוהל גיבוי ושחזור מידע הארגוני ינוהל לפי מהדורה עצמאית ומתעדכן באופן נפרד מנוהל אבטחת מידע, בפרקי זמן שונים, לפי הצורך והשינויים במבנה מערך הגיבוי הארגוני

6. אבטחת תקשורת ואינטרנט

6.1 תעבורת מידע

- 6.1.1 כל רשות מקומית תתקין ותשתמש דרך קבע בכלים מובנים ב"חומת האש" (Firewall) לצורך ניתוח פעילות ואירועים חריגים.
- 6.1.2 כל רשות מקומית תתקין ותשתמש דרך קבע בכלים טכנולוגיים המאפשרים שליטה ובקרה על רשתות התקשורת ומעקב לאחר זרימת המידע ואירועים חריגים במערכת המחשוב של הארגון.
- 6.1.3 כל הציוד האקטיבי, ממנו מורכבת רשת התקשורת הארגונית, יכלול יכולות ניהול תעבורה, תמיכה ברשתות וירטואליות (VLAN) וניהול משתמשים. סיסמאות המשתמשים יהיו באורך של 10 תווים לפחות ויוחלפו באופן ידני אחת לשנתיים.

6.2 התחברות מרחוק

- 6.2.1 במקרה של העברת מידע בין משרדי הרשות המקומית לבין בית העובד או עבודה על מחשבי ארגון מרחוק, באמצעות האינטרנט, יידרשו כתנאי לתקשורת זו, בין היתר, רכישה ותפעול של האמצעים האלה:
- 6.2.1.1 פתרונות תוכנה להתחברות מרחוק מאובטחים, מוכרים ומאושרים ע"י המנמ"ר.
- 6.2.1.2 התחברות לרשת הארגון תבצע בעזרת VPN CLIENT בלבד, אשר יותקן במחשבים "חיצוניים" באישור מנכ"ל הרשות.

6.3 מודעות העובדים

- 6.3.1 כל העובדים שהוגדרו על ידי הנהלת הרשות המקומית כבעלי זכות גישה לאינטרנט יאשרו בחתימת ידם על גבי טופס התחייבות משרדי-רשמי על התחייבותם למלא אחר ההנחיות הבאות:
- 6.3.1.1 קיים איסור מוחלט על פתיחת קבצים או תוכנות ממקורות שאינם מוכרים לעובד.
- 6.3.1.2 הורדת קבצים ותוכנות תיעשה רק אל Disk-On-Key אשר יועבר ל"עמדת בדיקה ייעודית" לגילוי פגעי אינטרנט, או לאישור "ניקינגם".
- 6.3.1.3 העובד לא ייעשה שימוש ביישומים מסוג JAVA או ACTIV-X האסורים לשימוש מאובטח ברשת האינטרנט.
- 6.3.1.4 דואר אלקטרוני ממקור חדש או לא מזוהה – אין לפתוח בשום אופן! הודעות ממקור לא ידוע עלולות להופיע בצורה אקראית בתיבת הדואר הנכנס. לגבי כל הודעה מסוג זה, יש להתייעץ עם מנהל מחשוב. גם אם נראה כי הודעת האזהרה הגיעה מהבנק ומחייבת ליצור קשר עם הסניף לבירור, יש להימנע להיכנס לקישור, לשלוח אימייל ו/או להתקשר למספרים המופיעים בהודעת האימייל עצמה.
- 6.3.1.5 יש להקפיד לא לפרסם מידע החושף את הארגון באינטרנט וברשתות חברתיות Facebook, Instagram, Twitter, וכדומה.
- 6.3.1.6 אין לשלוח בדואר אלקטרוני מידע מסווג/רגיש הכולל פרטים אישיים של התושבים והעובדים, פרטים פיננסיים של הרשות המקומית ותושביה וכיו"ב.
- 6.3.1.7 ממונה האבטחה יקיים בהתאם לתכנית עבודה שתאושר מראש הדרכות לעובדי המועצה לצורך הגברת מודעות אחת לשנה.



6.4 אינטרנט אלחוטי

- 6.4.1 חל איסור מוחלט להתחבר לרשת אלחוטית (Wi-Fi) לא מוצפנת בסיסמה. אין להתחבר לרשתות אלחוטיות לא מוכרות.
- 6.4.2 בכל מקרה של גלישה באינטרנט מחוץ למשרדי הרשות, יש להעדיף גלישה דרך הטלפון הסלולארי – נקודת גישה חמה (Tethering Hotspot).