כתובת לקבלת דואר:
משרד ראש הממשלה, רח' קפלן 3, ירושלים
טלפון 03-7450892, פקס 03-7450820

בלמ"ס

TLP: **לבן**



**<u>עקרונות הפעולה של המרכז הלאומי לסיוע בהתמודדות עם איומי סייבר</u>**

## 1. הגדרות

"**אירוע סייבר**" – הפרה או איום ממשי בהפרה של מדיניות הגנת סייבר במערכת ממוחשבת או פגיעה בשימוש במערכת ממוחשבת כפי שתוכננה, או באבטחתה, ובכלל זה:

1. שיבוש פעולתו התקינה של מחשב או הפרעה לשימוש בו;
2. מחיקת חומר מחשב , גרימה לשינוי בו, שיבושו בכל דרך אחת או הפרעה לשימוש בו;
3. איחסון מידע כוזב במחשב או הצגת פלט כוזב; "מידע כוזב" ו- "פלט כוזב" – "מידע או פלט שיש בהם כדי להטעות, בהתאם למטרות השימוש בהם".
4. חדירה שלא כדין לחומר מחשב;
5. האזנת סתר לתקשורת בין מחשבים;
6. חשיפה של מידע השמור במחשב לגורם שאינו מורשה לצפות בו.

"**גורמים עמם יש שיתופי פעולה**": גורמים העוסקים בתחום הגנת הסייבר שהמרכז משתף עמם פעולה במסגרת ייעודו ובכללם גופים מקבילים בעולם, קהילת הביטחון, משטרת ישראל, רמו"ט במשרד המשפטים, פורומים בינלאומיים, חברות תקשורת, מחשוב והגנת סייבר גלובליות.

"**הגנת סייבר**" – מכלול הפעולות למניעה, לנטרול, לחקירה ולהתמודדות עם איומי סייבר ואירועי סייבר, ולצמצום השפעתם והנזק הנגרם מהם, וזאת בטרם התרחשותם, במהלכם ולאחריהם.

"**המרכז**" – מרכז סיוע להתמודדות עם איומי סייבר המוקם במסגרת הרשות;

"**הרשות**" – הרשות הלאומית להגנת הסייבר בהתאם להחלטת ממשלה 2444 בנושא "קידום ההיערכות הלאומית להגנת סייבר" מיום 15.02.15;

"**מידע בעל ערך אבטחתי**" (actionable information): כל אחד מאלה:

א. **סממנים (indicators)** - נתונים אודות פעילות אשר ממנה ניתן להסיק כי התרחש, עלול להתרחש או מתרחש אירוע סייבר, [ובכלל זה מידע היקפי הנוגע לגילוי, זיהוי וחקירה של איומים ואירועים בדגש על מידע טכנולוגי גולמי];

ב. **חולשות (Vulnerabilities)** – תורפות במערכות ממוחשבת או רכיביהן או בנהלים הקשורים אליהן אשר ניתן לנצלן בכדי לייצר אירוע סייבר;

ג. **איומים (Threats)** – איום להתרחשות אירוע סייבר;

ד. **פוגענים ונוזקות (Artifacts and Malwares)** – יכולות וכלים אשר נעשה בהם שימוש כדי לנצל חולשה.

ה. **מתודולוגיות וכלי התמודדות עם איומי סייבר** – מתודולוגיות, יכולות וכלים לצורך זיהוי איומי סייבר, דרכי התמודדות והכלה של אירועי סייבר.

כתובת לקבלת דואר:
משרד ראש הממשלה, רח' קפלן 3, ירושלים
טלפון 03-7450892, פקס 03-7450820



**"מידע לא מזוהה"** : מידע, ובכלל זה מידע מוגן, שלא ניתן באמצעים סבירים לזהות את היחיד או הארגון שהוא מתאר.

**"מידע מוגן"** – כל אחד מאלה :

1. מידע שחוק הגנת הפרטיות, התשמ"א-1981 חל עליו לעניין יחיד ;
2. מידע אודות ארגון שאינו נחלת הכלל ;
3. סודות מסחריים לפי חוק עוולות מסחריות.

**"מערכות המרכז"** – מערכות החומרה והתוכנה המשמשות לביצוע משימות המרכז.

**"קהלי יעד" (Constituencies)** - גורמים במשק שהמרכז מסייע להם במסגרת ייעודו ובכלל זה, ארגונים וחברות מכל המגזרים ; משרדי ממשלה ; ספקי תקשורת ואינטרנט ; חברות מוצרים, ייעוץ ושירותים בהגנת סייבר ; בעלי מקצוע בהגנת סייבר ; הציבור הרחב.

**2. ייעוד**

א. המרכז מוקם במסגרת הרשות וכחלק מייעודה.

ב. ייעוד המרכז הינו סיוע להתמודדות עם איומי סייבר עבור כלל המשק, ובכלל זה :

1. שיפור החוסן ההגנתי בסייבר.
2. סיוע בטיפול באיומי סייבר.
3. סיוע בטיפול באירועי סייבר.
4. ריכוז ושיתוף מידע בעל ערך הגנתי עם כלל הגורמים במשק.
5. להוות נקודת ממשק מרכזית בין גופי הביטחון לבין הגורמים במשק לצרכי הגנת הסייבר.

ג. המרכז לא יבצע פעולות שאינן קשורות בייעוד זה.

ד. המרכז יקפיד על איזון בין צורכי הגנת הסייבר לבין הגנה על זכויות יסוד בעת מימוש ייעודו.

ה. רשימת שירותי המרכז מופיעה בנספח א' ומתעדכנת מעת לעת באתר האינטרנט של הרשות : www.ncsa.gov.il.

3. **אחריותיות וניהול תקין**– accountability

א. האחריות הכוללת לקיום עקרונות אלה במסגרת פעילות הרשות הינה של ראש הרשות, כמפורט להלן :

1. מינוי מנהל המרכז מבין עובדי הרשות.
2. פיקוח על כתיבת נהלי העבודה המפורטים למרכז בהתאם לעקרונות אלה, ובחינת הצורך בעדכונם לפחות אחת לשנה בהתאם לפעילות המרכז.
3. הקמה של מנגנוני פיקוח לקיום העקרונות.

ב. עקרונות אלה ימומשו בפעילות המרכז תוך שימוש בשיטות וכלים המפורטים להלן, לפי העניין :

1. עיצוב טכנולוגי (by design) של מערכות המרכז.

כתובת לקבלת דואר:
משרד ראש הממשלה, רח' קפלן 3, ירושלים
טלפון 03-7450892, פקס 03-7450820



2. בקרות טכנולוגיות במערכות המרכז ותהליכי עבודה תומכים.
3. נהלי עבודה מסדירים.

ג. ראש הרשות ימנה עובד מבין עובדי הרשות, בעל הכשרה מתאימה, לפקח על קיום עקרונות אלה לגבי מידע מוגן (להלן – הממונה), וביצוע בקרה למימושה.

ד. ראש הרשות יוודא כי לממונה יש את האמצעים הנדרשים למילוי תפקידו. הממונה יהיה גם "ממונה הפרטיות" לעניין מידע מוגן לפי חוק הגנת הפרטיות.

ה. ראש הרשות יגיש אחת לשנה דין וחשבון על קיום עקרונות אלה לראש מערך הסייבר הלאומי.

**4. קבלה ואיסוף של מידע**

א. המרכז יאסוף מידע בעל ערך אבטחתי לצרכי ייעוד המרכז.

ב. המרכז יאסוף מידע ממקורות אלה:

1. מגורם מקהל היעד לאחר שהתקיימו אלה:
   א. הוצגו לגורם עיקרי עקרונות אלה;
   ב. הוצגו לגורם תיאור פרוטוקול "רמזור" לעניין ההפצה לקהל היעד או פרוטוקול אחר כפי שייקבע לפי סעיף 7(ב) לעניין סיווג המידע, כמפורט בנספח ב'.
   ג. הגורם הסכים למסור את המידע בהתאם לעקרונות אלה.
   ד. אם במסגרת ההתקשרות עשוי להיאסף מידע מוגן שחוק הגנת הפרטיות, התשמ"א-1981 חל עליו לעניין יחיד, הגורם פרסם הודעה לעובדיו ולקוחותיו אודות שיתוף הפעולה עם המרכז הכולל העברת מידע בעל ערך אבטחתי מהארגון למרכז בהתאם לנוסח הודעה שהפיץ המרכז.
2. מגורמים עמם יש לו שיתוף פעולה.
3. מגורמים אשר הוטלה עליהם חובה למסור לו מידע.
4. כל מקור חוקי אחר.

ג. איסוף מידע המכיל מידע מוגן יהיה בהיקף המינימלי הנדרש לצורכי ייעוד המרכז. במידה שיתברר למרכז כי נאסף מידע שחוק הגנת הפרטיות, התשמ"א-1981 חל עליו לעניין יחיד, לא ייעשה בו כל שימוש והמידע יימחק, אלא אם התקיים אחד מאלה:

1. המרכז בירר כי איסוף המידע והשימוש בו נעשים בהסכמה של היחיד שהמידע אודותיו לפי חוק הגנת הפרטיות, התשמ"א-1981, בהתאם לרגישות המידע ואופן השימוש בו,
2. היועץ המשפטי של המרכז אישר כי שימוש במידע נדרש בדחיפות לשם התמודדות עם אירוע סייבר, וכי בנסיבות העניין, בשים לב לרגישות המידע ולחומרת האירוע, לא יהיה בשימוש במידע משום הפרה של הוראות חוק הגנת הפרטיות. ניתן אישור היועץ המשפטי לפי סעיף זה, ידווח על כך המרכז ליועץ המשפטי לממשלה.

**5. שמירת המידע במערכות המרכז**

כתובת לקבלת דואר:
משרד ראש הממשלה, רח' קפלן 3, ירושלים
טלפון 03-7450892, פקס 03-7450820



א. המרכז יישם כללי תיוג מידע שיאפשרו ציון רגישות המידע, רמת השיתוף שלו, והרשאות ביחס לשימוש בו.

ב. שמירת המידע תיעשה ככל הניתן באופן שהוא יהיה מידע לא מזוהה ;

ג. המרכז ינקוט שיטות ואמצעים להפקת מידע בעל ערך הגנתי ממידע מוגן עם קבלתו באופן המצמצם את הצורך בשמירת המידע המוגן הגולמי.

ד. מידע גולמי אשר יש אפשרות סבירה שהוא מכיל מידע מוגן יישמר בנפרד והגישה אליו תוגבל לתהליכים ועובדים ייעודים ברשות.

ה. מידע מוגן יישמר לפרק הזמן המינימלי הנדרש באופן סביר לשימוש בו.

**6. עיבוד מידע**

א. פעילות העיבוד והתיחקור של המידע במערכות המרכז תמוקד באיתור והפקה של מידע בעל ערך אבטחתי, ופעולות נדרשות לצורך הגנת הסייבר.

ב. המידע לא יעובד למטרות שאינן במסגרת ייעוד המרכז והרשות.

**7. הפצת מידע לקהל היעד**

א. המרכז יפיץ מידע בעל ערך אבטחתי בלבד לקהל היעד.

ב. המרכז יפיץ מידע לקהל היעד בהתאם לפרוטוקול רמזור או פרוטוקול אחר כפי שיפרסם ה- CERT לציבור. בהתאם לכך, המרכז יפיץ לקהל היעד מידע אודות הגורם שדיווח אותו באופן לא מזוהה, אלא אם הגורם המדווח הסכים לכך.

ג. המרכז ינקוט אמצעים סבירים לבדיקת המהימנות של המידע המופץ.

ד. המרכז לא יהיה אחראי לאופן השימוש במידע המופץ במערכות הארגון המקבל.

ה. המרכז יפיץ מידע בעל ערך אבטחתי הכולל מידע מוגן שחוק הגנת הפרטיות חל עליו, רק בכפוף לתנאי סעיף 4(ג).

**8. הגנת הסייבר ואבטחת מידע בפעילות המרכז**

א. המרכז יעשה שימוש בטכנולוגיה, נהלים ושיטות שמטרתם הגנה על מערכות המרכז והמידע שבהן מפני שיבוש, שינוי או גישה לא מורשית, בשים לב לסיכונים הרלבנטים.

ב. עקרונות אלה יחולו גם על מערכות גיבוי והמידע שנשמר בהן.

**9. כוח אדם - הרשאות גישה ומידור**

א. מנהל המרכז יקבע הרשאות גישה למערכות המרכז על בסיס הגדרת תפקיד ( role based) ; הרשאת הגישה לכל תפקיד תהיה במידה הנדרשת לביצוע התפקיד בלבד.

ב. הרשאות גישה למידע יהיו ככל הניתן באופן שהוא יהיה מידע לא מזוהה, בשים לב לייעוד המרכז.

ג. במערכות המרכז ינוהל מנגנון תיעוד אוטומטי שיאפשר בקרה וביקורת על הגישה למידע במערכות המרכז.

כתובת לקבלת דואר:
משרד ראש הממשלה, רח' קפלן 3, ירושלים
טלפון 03-7450892, פקס 03-7450820



ד. ההרשאות יוקצו למערכות המרכז על פי הנחיות מנהל המרכז לאחר התייעצות עם הממונה, לאחר נקיטת אמצעים מקובלים לבדיקת ההתאמה שלהם לגישה ושימוש במערכות.

ה. הממונה על מידע מוגן יקיים הדרכות לעובדים בנושא החובות לפי עקרונות אלה והדינים החלים על מידע מוגן.

**10. בקרות**

א. המרכז יישם, ככל הניתן, מנגנונים אוטומטים במערכותיו שיאפשרו בקרה על קיום העקרונות והנהלים לפיהם.

ב. הממונה יפקח על מנגנוני הבקרה לצורך איתור אירועים של חשש לשימוש לרעה.

11. **שקיפות בפעילות עיבוד המידע של המרכז**

א. עקרונות אלה יועמדו לעיון הציבור באתר הרשות.

ב. המרכז יפרסם לגורמים עמם יש לו שיתוף פעולה המלצות לעניין אופן יידוע עובדיהם ולקוחותיהם אודות שיתוף הפעולה עם המרכז

**נספח א' – שירותי המרכז – מרץ 2015**

**רשימת השירותים מתעדכנת מעת לעת באתר הרשות:** www.ncsa.gov.il

**שירותים**

CERT-IL מיועד להציע מגוון שירותים שיינתנו בהתאם למאפייני האיום, האירוע והגורמים בקהלי היעד ובכפוף לכללי פעילותו. סוגיהם מוגדרים לפי המתודולוגיה שפותחה על ידי הגופים המובילים בעולם:

- שירותים ריאקטיביים – מוצעים לאור אירוע, אינדיקציה, דיווח או בקשה פרטנית, ובכלל זה: התרעות ואזהרות, סיוע בטיפול באירועים, מחקר טכנולוגי לזיהוי וניתוח פוגענים.
- שירותים פרואקטיביים – מספקים סיוע ומידע לשיפור רמת המוכנות וההגנה למול אירועים עתידיים, ובכלל זה: הסברה, הדרכה ותרגול, בדיקות יזומות לגילוי איומים.
- שירותים משלימים בניהול האבטחה.

**כתובת לקבלת דואר:**
משרד ראש הממשלה, רח' קפלן 3, ירושלים
טלפון 03-7450892, פקס 03-7450820

בלמ"ס

TLP: **לבן**



נספח ב'

**שיטת הרמזור הינה שיטה מקובלת לסיווג מידע רגיש שאינו מסווג מבחינה ביטחונית. מטרתה להקל על שיתוף מידע תוך הגדרת מגבלות והתניות לגבי הפצתו. סימון זה יוצר מוסכמה בין השותפים לבין אופן השימוש הנאות במידע, על מנת לאפשר העברת מידע הגנתי חשוב לכל הגורמים הרלוונטיים תוך מזעור החשש לפגישה בגורם המשתף**

| ייעוד הסיווג | הסיווג | מגבלות השיתוף של הגורם המקבל |
|---|---|---|
| מקרים בהם המידע הינו בעל ערך הגנתי אפקטיבי לגורמים נוספים ועלול להוביל לפגיעה בפרטיות, במוניטין או בפעילות אחרת של הגורם המשתף אם ייעשה בו שימוש לרעה | אדום | אין לשתף מידע המסווג "אדום" עם אף גורם מחוץ לקבוצת הנמענים המקורית |
| מקרים בהם שימוש אפקטיבי במידע מצריך שיתוף גורמים נוספים, אך הרחבת התפוצה מעבר לכך עלולה לפגוע בפרטיות, במוניטין או בפעילות הגורם המשתף | צהוב | ניתן לשתף מידע המסווג "צהוב" רק עם גורמים באותו הארגון, ורק במידה הנדרשת לטובת מתן מענה אפקטיבי |
| מקרים בהם המידע עשוי להועיל לגורמים רבים ושיתופו אינו כרוך בסיכון לגורם המשתף | ירוק | ניתן לשתף מידע המסווג "ירוק" עם כל הגורמים העשויים לעשות בו שימוש מועיל. עם זאת, אין לשתפו בערוצים פומביים, דוגמת אתרי אינטרנט, רשתות חברתיות ואמצעי תקשורת המונים |
| מקרים בהם נראה כי קיים סיכון מינימלי או לא קיים סיכון כלל בהפצה של מידע, בכפוף לזכויות יוצרים | לבן | ניתן לשתף מידע המסווג "לבן" עם כל קבוצת נמענים, לרבות ערוצים פומביים |