



אבטחת מידע ופרטיות בעמותות

26.12.2023

נבחרת
הדירקטורים
החברתית
להתחבר. לעשות. להשפיע.

intel®

הג'וינט 

ג'וינט - אלכא | יעילות ומועילות המערכות הציבוריות

הג'וינט



באלכא אנו מאמינים ש:

Better systems



Better services



Better lives

לכן אנו פועלים ל:

חיזוק יכולת המערכות הציבוריות לספק שירותים חברתיים לתושבי ישראל, ביעילות ומועילות.

נבחרת הדירקטורים החברתית

מיזם מבית ג'וינט-אלכא המהווה בית מקצועי לדירקטוריונים חברתיים; מאגר לאומי של מנהלות ומנהלים בכירים ממגוון תחומים ומומחיות, עם מוטיבציה לקדם השפעה חברתית ולשמש בהתנדבות כדירקטורים חברתיים. לצד זאת, מרכז ידע המפתח ומנגיש ידע וכלים הדרושים לבעלי תפקידים בדירקטוריון חברתי.



התמקצעות



מנהיגות

MEET-UP 2023 ליו"ר, דירקטוריות, ומנכ"ל ארגונים חברתיים

שריינו ביומן:



15.2

עמדות ותפיסות תפקיד
בפיתוח משאבים

10.5

משוב יו"ר-מנכ"ל

10.9

הקצבת כהונה וקדנציה

1.11

דירקטוריון בחירום - שיח משותף

26.12

אבטחת מידע במגזר החברתי

1

אבטחת מידע ופרטיות
למה הנושא נבחר ולמה
זה חשוב?

2

צוללים לעומק
הצגת סוגיות נבחרות –
איך לנהל ולשמור על
מידע ופרטיות

3

סיכום וצידה לדרך
איך ניתן בפועל לקדם
את הנושא –
המלצות יישומיות

7 הכובעים לתפקיד << דירקטוריון אפקטיבי

✓ קביעת חזון ואסטרטגיה

✓ אישור תקציב ותכניות עבודה

✓ גיוס ופיתוח משאבים

✓ **מעקב ובקרה**

✓ ייצוג והעצמת העמותה

✓ גיוס, ליווי והערכת המנכ"ל

✓ פיתוח צוות הדירקטוריון

1

מאיה יצחקי

מומחית אבטחת מידע
והערכת סיכונים עם
התמקצעות ברכישות
ומיזוגים, אינטל ישראל

2

מישל לוי

מנהלת צוות תגובה
למתקפות סייבר וצוות
מודיעין סייבר של
אינטל ישראל; מייעצת
לעמותות בענייני
אבטחת מידע
ודיגיטליזציה

3

יפעת סימינובסקי
מומחית פרטיות
ומובילת הגנת
הפרטיות באינטל
ישראל

העידן הדיגיטלי מציב אתגרים חדשים.
לנוכח צרכי איסוף, עיבוד ושימוש במידע
- מעלה שאלות על אופן יישום חוק הגנת
הפרטיות ותקנותיו.

בין היתר לגבי רישום המידע, הגדרת
רמת הסודיות שלו, מי אחראי על מידע
זה, למי מידע זה נגיש וכיצד לשמור עליו.



קביעת הפרה לעמותת טף לאימוץ בינארצי

תאריך פרסום: 17.10.2017

נושא: [מידע לציבור הרחב](#), [חברות ועסקים](#), [פעילות](#)[אכיפה](#)

מחלקת האכיפה של הרשות להגנת הפרטיות קיימה הליך פיקוח לבירור אירוע דלף מידע אישי רגיש משרת מחשב של עמותת טף – (עמותה לאימוץ בינארצי) ע"ר.

TheMarker | TechNation

קורבן נוסף: אחת העמותות הגדולות בארץ נפגעה במתקפת האקרים

בישראל אירעו בתקופה האחרונה כמה מתקפות סייבר, שמאחוריהן עומדים ככל הנראה גורמים איראניים ■ בעמותת מטב טוענים כי המתקפה "לא פגעה בהתנהלות השוטפת"

ללא אבטחה

מי אחראי על דליפת מידע רפואי של בנות שרות לאומי לרשת?

ברשות להגנת הפרטיות חוקרים כיצד ליקוי חמור באבטחת המידע בעמותת עמינדב, אגודה תורנית להתנדבות, הוביל לדליפת המידע הרגיש לרשת

האיום החיצוני על עמותות

- האקרים פיננסים - קבוצות שמעוניינות בכסף
- גורמים מדיניים
- גורמים אידיאולוגים מתחרים
- צד ג' - תוכנות ושירותים חיצוניים

האיום הפנימי על עמותות

- דליפת מידע
- הזלגת מידע
- מעילה באמון
- צד ג' - תוכנות ושירותים חיצוניים

אבטחת מידע ופרטיות - אחים ולא תאומים

פרטיות



מתמקדת במשילות ובאחריות על המידע אישי הנאסף ומעובד על ידי הארגון ואופן הטיפול בו לאורך מעגל החיים של המידע

אבטחת מידע



מתמקדת בהגנה על מערכות המידע של הארגון מאיומי תקיפה

אבטחת מידע / הגנת סייבר ופרטיות

עובדים יחד כדי לייצר וליישם את אמצעי ההגנה הנדרשים לעיבוד מידע אישי בצורה מאובטחת, וכדי לטפל במידע אישי בהתאם לחוקים ולרגולציה החלים על מידע זה.

הגנת פרטיות ומידע אישי - מושגי בסיס

מידע אישי:

- לפי החוק הישראלי: נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו.
- בפועל - פרשנות רחבה. כלל אצבע: כל מידע שניתן לשייך לאדם, או לזהות אותו באמצעותו, בין אם ישירות או על ידי קישור לנתונים נוספים.
- מידע אישי יכול להוות גם מידע רגיש.
- באופן כללי, הזכות לפרטיות (בהקשרי מידע) מתייחסת לזכותו של אדם לשליטה על המידע האישי שלו ועל אופן השימוש בו.
- פגיעה בפרטיות - שימוש בידיעה על ענייניו הפרטיים של אדם או מסירתה לאחר, שלא למטרה לשמה נמסרה; הפרה של חובת סודיות שנקבעה בדין או בהסכם (מפורש או משתמע) לגבי ענייניו הפרטיים של אדם; פרסום תצלום של אדם בנסיבות בהן הפרסום עלול לבזותו או להשפילו; ועוד.
- תאימות לפרטיות - (Privacy Compliance) מתייחסת לאופן בו ארגונים עומדים בחובות הרגולטוריות המוטלות עליהם בנוגע לעיסוק במידע אישי. איסופו, שימוש בו, גישה אליו, שיתופו, שמירתו, עיבודו ומחיקתו.

הנהלת עמותות והגנת פרטיות

- כמי שאמונים על סיוע לאוכלוסיות פגיעות ומוחלשות, וממונים על פעילות המערבת מידע אישי רגיש, אתם מצופים לפעול באחריות ובהתאם לרגולציה בכל הנוגע לשימוש במידע אישי ולשמירה עליו.
- פעלו תמיד עם חשיבה על הגנת הפרטיות.
- סייעו להגביר מודעות ותאימות בעמותה ובקרבת המתנדבים.
- התייחסו למידע אישי כמשאב חיוני של העמותה. בהתאם, הכירו -
 - ✓ איזה מידע פרטי אתם אוספים, שומרים ומעבדים
 - ✓ ממי המידע נאסף
 - ✓ כיצד המידע נאסף
 - ✓ היכן הוא נשמר
 - ✓ למה הוא משמש וכיצד
 - ✓ האם הוא מועבר על ידכם לגורם שלישי, ולאיזה צורך

הגנת הפרטיות בישראל

- בישראל הזכות לפרטיות הינה זכות יסוד לפי חוק יסוד כבוד האדם וחירותו.
- החוק המרכזי המסדיר את הנושא הוא **חוק הגנת הפרטיות תשמ"א-1981** ותקנותיו. ישנם הסדרים רגולטוריים נוספים, ייעודים לתחומים ספציפיים (למשל בתחום הבריאות).

איסוף מידע מוגן פרטיות ושימוש בו יתבצעו רק בהסכמה או בהתאם לסמכות חוקית.

- פגיעה בפרטיות היא עוולה אזרחית נזיקית, ועלולה להוות גם עבירה פלילית.
- **חובת רישום מאגרי מידע:** כל מאגר המכיל מידע רגיש, כולל מידע על אנשים שלא נמסר על ידם או בהסכמתם, מיכל מידע על יותר מ 10,000 איש, ועוד. (חובה זו תצומצם משמעותית אם הצעת תיקון החוק תאושר).
- **חובת אבטחת מאגרי מידע:** בהתאם לתקנות הגנת הפרטיות (אבטחת מידע): כוללות בין היתר חובת הסדרה של יחסים בין בעל המאגר לבין מחזיק/מיקור חוץ לעיבוד מידע, תיעוד מסמכי מאגר, נהלי אבטחת מידע, בקורות תקופתיות וביצוע מיפוי מערכות וסקר סיכונים, דיווח לרשות על אירוע אבטחת מידע, בחינה אחת לשנה שהמאגר לא מכיל מידע עודף, ועוד.
- **הנחיות הרשות להגנת הפרטיות:** מפורסמות באתר הרשות.

הגנת פרטיות - המלצות מעשיות

משילות מידע ואחריות

איזה מידע נאסף, אופן ניהולו, שמירתו ושימוש בו, מדיניות, נהלי עבודה וקבלת החלטות, פלטפורמות טכנולוגיות (שימו לב לרישוי!) (שימו לב לרישוי!)

צמצום מידע

אספו והשתמשו אך ורק במידע המינימלי הנדרש לצורך המטרה. אל תאספו מידע עודף ואל תשתמשו בו

צמידות מטרה

הקפידו לעשות שימוש במידע אך ורק למטרה לשמו נאסף ושתוארה בהודעה

יידוע ושקיפות

ספקו מידע בפלטפורמה הרלוונטית לפעילות (אתר/שאלון/דיוור/וכו) וטרם איסוף המידע - האם מסירת המידע הינה חובה לפי חוק, איזה מידע נאסף, לאיזה מטרת ישמש המידע, האם יועבר לגורמים נוספים. ספקו קישור למדיניות הפרטיות שלכם ואמצעי ליצירת קשר

אבטחת מידע

הגדרת רגישות המידע ואבטחתו בהתאם. יישום מרכיבי אבטחת מידע והגנת סייבר בסטנדרט מקובל ובהתאם לדרישות הרגולציה

מחיקת מידע

מחקו את המידע האישי כאשר אין בו צורך יותר - בהתאם למדיניות תקופות שמירת מידע עליה יוחלט לפי סוגי המידע

הגבלת גישה וניהול הרשאות גישה

ודאו כי הגישה למידע מוגבלת אך ורק למי שנדרש לה לצורך ביצוע המטרה "הצורך לדעת" (Need to Know)

העלאת מודעות עובדים ומתנדבים והפצת נהלים והנחיות בנוגע למידע פרטי

בקרות נוספות בהתאם לרגולציה ולהנחיות ייעודיות החלות על פעילות העמותה בהתאם למגזר הפעילות (למשל - בריאות, חינוך, וכו')

המדריך המלא ליישום תקנות הגנת הפרטיות (אבטחת מידע)

במדריך הבא תמצאו מידע אודות כלל סעיפי תקנות הגנת הפרטיות (אבטחת מידע)



1. מהי אבטחת מידע?
2. על מי חלות התקנות?
3. על אילו מאגרים חלה רמת האבטחה הבסיסית? הבינונית או הגבוהה?
4. מסמך הגדרות המאגר - תקנה 2
5. ממונה על אבטחת מידע - תקנה 3
6. נוהל אבטחה - תקנה 4
7. מיפוי מערכות המאגר וביצוע סקר סיכונים - תקנה 5
8. אבטחה פיזית וסביבתית - תקנה 6
9. אבטחת מידע בניהול כוח אדם - תקנה 7
10. ניהול הרשאות הגישה - תקנה 8
11. זיהוי ואימות - תקנה 9
12. בקרה ותיעוד גישה - תקנה 10
13. תיעוד של אירועי אבטחה - תקנה 11
14. התקנים ניידיים - תקנה 12
15. ניהול מאובטח ומעודכן של מערכות המאגר - תקנה 13
16. אבטחת תקשורת - תקנה 14
17. מיקור חוץ - תקנה 15
18. ביקורות תקופתיות - תקנה 16
19. משך שמירת נתוני האבטחה? - תקנה 17
20. גיבוי ושחזור נתוני אבטחה - תקנה 18
21. האחריות לאבטחת המידע - תקנה 19
22. רגולציה ותקנים מקבילים - תקנה 20

תקנות הגנת הפרטיות (אבטחת מידע)

הפערים בעמותות

מידע מפוזר



מתנדבים.ות לא קבועים.ות



חוסר ידע טכנולוגי ואבטחת מידע



היעדר מדיניות אבטחת מידע



מאיפה להתחיל?

| מערכות | מידע | אנשים | מיפוי |
|--|--|--|--|
| (1) איזה מערכות יש לי של הארגון (2) איזה מערכות צד שלישי, ספקים ושירותים (3) מיפוי תנאי השירות | (1) מה המידע שיש לי : ✓ תיוג – מה רגיש? ✓ תיוג לפי רמות הרגישות (2) רישום מאגר המידע (3) איפה המידע כיום (4) למי יש גישה למידע (5) כיצד מתבצעת הגישה | זיהוי ורישום • עובדים.ות • מתנדבים.ות קבועים.ות • מתנדבים זמנים (ומשך ההתנדבות) | (1) כתיבת המדיניות- ✓ מה נדרש מהעובדים, מתנדבים והועד- בכניסה לארגון ויציאה. ✓ דרישות סף- הדרכות? חתימת הסכם מתנדב? (2) מינוי אחראי.ת אבטחת המידע (3) מה עושים במקרה של חשד\אירוע סייבר |
| (1) בדיקת מדיניות הספקים וקביעת נהלים לשימוש בתוכנות, כלים ושירותים- ✓ מי אחראי.ת המערכת ✓ כל כמה זמן עושים ביקורת ✓ מיקסום אמצעי אבטחת המידע (2) בחירה של אמצעי אבטחת המידע | (1) קביעה איפה, מי ואיך נגשים למידע. (2) לכמה זמן שומרים את המידע | (1) יצירת מסמך הסכם מתנדב.ת\עובד.ת (2) הצגת התוכנית | (1) יצירת סביבה עבודה פיזית ו\או וירטואלית לארגון. (2) צמצום ספקים- מרכז שירותים (3) אמצעי אבטחת המידע (4) איסוף לוגים והתרעות (5) תיעוד אירועים ודיווח על פי הצורך (6) ביצוע גיבויים |
| (1) יצירת סביבה עבודה פיזית ו\או וירטואלית לארגון. (2) צמצום ספקים- מרכז שירותים (3) אמצעי אבטחת המידע (4) איסוף לוגים והתרעות (5) תיעוד אירועים ודיווח על פי הצורך (6) ביצוע גיבויים | (1) ריכוז המידע במשאבי העמותה\ארגון (2) תיוג המידע וצמצום מידע (3) מחיקת מידע (4) צמצום גישה | (1) יצירת מסמך הסכם מתנדב.ת\עובד.ת (2) הצגת התוכנית | (1) יצירת סביבה עבודה פיזית ו\או וירטואלית לארגון. (2) צמצום ספקים- מרכז שירותים (3) אמצעי אבטחת המידע (4) איסוף לוגים והתרעות (5) תיעוד אירועים ודיווח על פי הצורך (6) ביצוע גיבויים |



הדרכות ומודעות

- הדרכת תחילת העסקה
- הדרכת סוף העסקה
- הדרכה שנתית
 - מודעות אבטחת מידע
 - תרגול
- הדרכות על מערכות ושימוש ← על פי הצורך

על מה לא עברנו כאן?

○ מוצרי אבטחת מידע

- תלוי בצרכים של העמותה\ארגון

- פיזים ווירטואלים

- ניצול המנגנונים של כל תוכנה\מוצר

○ תשתיות לשמירת מידע וניטור

○ מה עושים באירוע אמת

איך לגשת ולשמור מידע

| תוכנות | ישיבות וירטואליות | שלב ההזדהות | אחסון מידע | אימייל וכלי שיתוף |
|--|--|---|--|---|
| כל התוכנות ושירותי הענן שהעמותה משתמשת בהם יהיו ברשיון לעמותה. וזאת על מנת להגן על המידע, לקבל עדכוני אבטחה ולמנוע התקפות סיבר שמגיעות מחברה צד שלישי. | ישיבות וירטואליות יעשו בכלים מאושרים עם רשיון. לוודא שאתם מכירים את מי שעלה לישיבה ואם משתפים מידע לוודא שהם מאוחסנים רק לשטח אחסון המידע שמאושר ע"י העמותה. | ההמלצה היא שחיבור למידע של העמותה יבוצע בתהליך דו שלבי. סיסמא שאתם מכירים וקוד חד פעמי שישלח לנייד או למייל העסקי שלכם. | המידע של העמותה ישמר בצורה מאובטחת באמצעי האחסון עם רשיון של העמותה. כמו OneDrive, Google drive. לא להוריד מידע לשטחי אחסון שלא מורשים ע"י העמותה כמו אינטרט קפה, מחשבי עבודה.... גישה למידע תיהיה רק למי שיש לו צורך להגיע למידע. | ההמלצה להשתמש בתוכנות מורשות של גוגל או מיקרוסופט. G-workspace/ O365 for NGO (שכולל גיבוי חינומי) |

האחריות החוקית על המידע שבשימוש העמותה היא של העמותה, ולכן ההמלצה היא להשתמש בתוכנות חוקיות ולשמור על המידע רק באמצעי אחסון ידועים, מאובטחים ומנוהלים וזאת על מנת למנוע זליגת מידע או הידבקות בוירוסים.

קישורים שימושיים עבורכם ועבור העמותות

1. חוק הגנת הפרטיות, הכולל בתוכו רשימת חובות שבהן צריכות עמותות לעמוד -
https://www.nevo.co.il/law_html/law00/71631.htm (פרק ב' עוסק בהגנה על הפרטיות במאגרי מידע)
2. אתר הרשות להגנת הפרטיות, המרכז בתוכו הנחיות ייעודיות לכל סקטור, ארגזי כלים, ומקום לדיווח במקרה והתרחש אירוע אבטחת מידע –
https://www.gov.il/he/departments/the_privacy_protection_authority/govil-landing-page
שימו לב ❤️ - במקרה של דליפה חובה לדווח לרשות להגנת הפרטיות.
3. מערך הסייבר הלאומי בחיוג מהיר 119
4. [מערך הסייבר הלאומי](#)
5. [Google - G-workspace for NGO](#)
6. [Microsoft - O365 for NGO](#)

ארגז כלים לדרך <<

פריטי תוכן חדשים

הקצבת כהונה וקדנציה בדירקטוריון
ריענון הרכב הדירקטוריון משמעו התאמתו לאתגרי התקופה. אין זה בא...

**הערכת יו"ר-מנכ"ל של ארגון חברתי |
"בין משימות ליחסים"**
ניהולם והובלתם של ארגונים להצלחה והשגת כלל מטרותיהם היא משימה...

**עמדות, אמונות ותפיסת תפקיד | פיתוח
וגיוס משאבים בדירקטוריון**
כולנו יודעים שפיתוח וגיוס משאבים זה החמצן של העמותה. ובכל...

**מחקר דירקטוריונים חברתיים ארצי
2021**
בשנת 2021 ערכנו מחקר בקרב מנכ"לים וחברי דירקטוריון בארגונים חברתיים...



פיתוח משאבים



הארגון החברתי



המעטפת הרגולטורית



Find Us >>



[Link](#)



[Link](#)



[Link](#)



[Link](#)

נבחרת
הדייקטורים
החברתית
להתחבר. לעשות. להשפיע.



דירקטוריון מצוין הוא
המנוף של העמותה.