

# מפת"ח • MethodA

## תשתית אבטחת מידע

מצגת מנהלים



© כל הזכויות שמורות

[www.methoda.com](http://www.methoda.com)

בחירה באיכות  
**מתודה**



# קייט תשתית אבטחת מידע

❖ הקייט מיועד לסייע בפרויקט שיפור תשתיות אבטחת

המידע בארגון

❖ השיפור חייב לנבוע מצורכי מערכות המידע

❖ הפרויקט מטפל ברמת הארגון בהיבטים של:

○ אבטחה פיזית

○ מדיניות ונהלים

○ תהליכים הקשורים לכוח אדם

❖ הקייט סוקר היבטים מיוחדים של פרויקט מסוג זה ואת

השלכותיהם על מחזור החיים ועל עץ המערכת

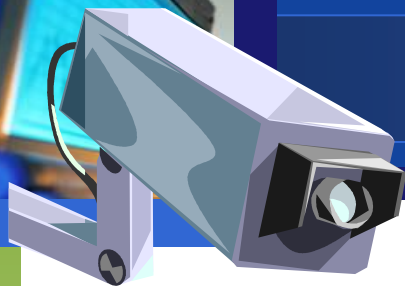
# תועלות השימוש בקיט



❖ פרויקט תשתית אבטחת מידע לארגון  
הינו פרויקט מורכב, יקר, ומשפיע לרוחב  
כל הארגון. חשוב מאד להגדיר היטב את כל השלבים  
וההיבטים הפרויקטליים ע"מ להצליח בפן האבטחתי,  
בעלויות ובלו"ז.

❖ שימוש נכון בעץ המערכת המפורט בקיט זה, יחד עם  
הדגשים המתוארים בקיט, במהלך מחזור החיים של  
הפרויקט, יעזרו מאד להצלחת הפרויקט.

# אבטחת מערכות מידע

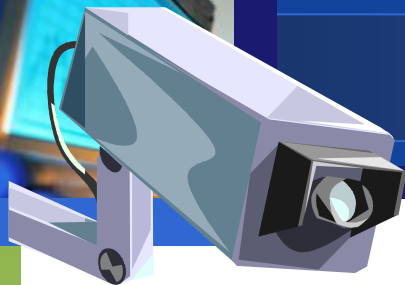


❖ שמירה על שלושה פרמטרים:

- חיסיון המידע (Confidentiality)
- זמינות מערכות המידע (Availability)
- שלמות המידע (Integrity)

❖ בארבע פעולות על המידע

- Create - יצירה\הוספה של מידע חדש
- Read – קריאה\שליפה של מידע
- Update – עדכון והכנסת שינויים
- Delete – מחיקה\ביטול של מידע



## ❖ נושא רחבי חוצה-ארגון המשלב:

- תהליכים ארגוניים (או"ש)
- יישומים – מידע עסקי
- פתרונות טכנולוגיים
- אנשים ובעלי תפקידים
- הנדסות שכנות: סיוע טכני

## ❖ במגוון רמות:

- האפליקציה הבודדת (פרויקט מיוחד)
- מדור\חטיבה בארגון
- תשתית כלל ארגונית

# נזקי פגיעה באבטחת המידע

## ❖ בעולם העסקי

- הפסדים כספיים
- מניעת השגת היעדים העסקיים
- לעיתים אף להתמוטטות הארגון

## ❖ בתחום הממשלתי/בטחוני

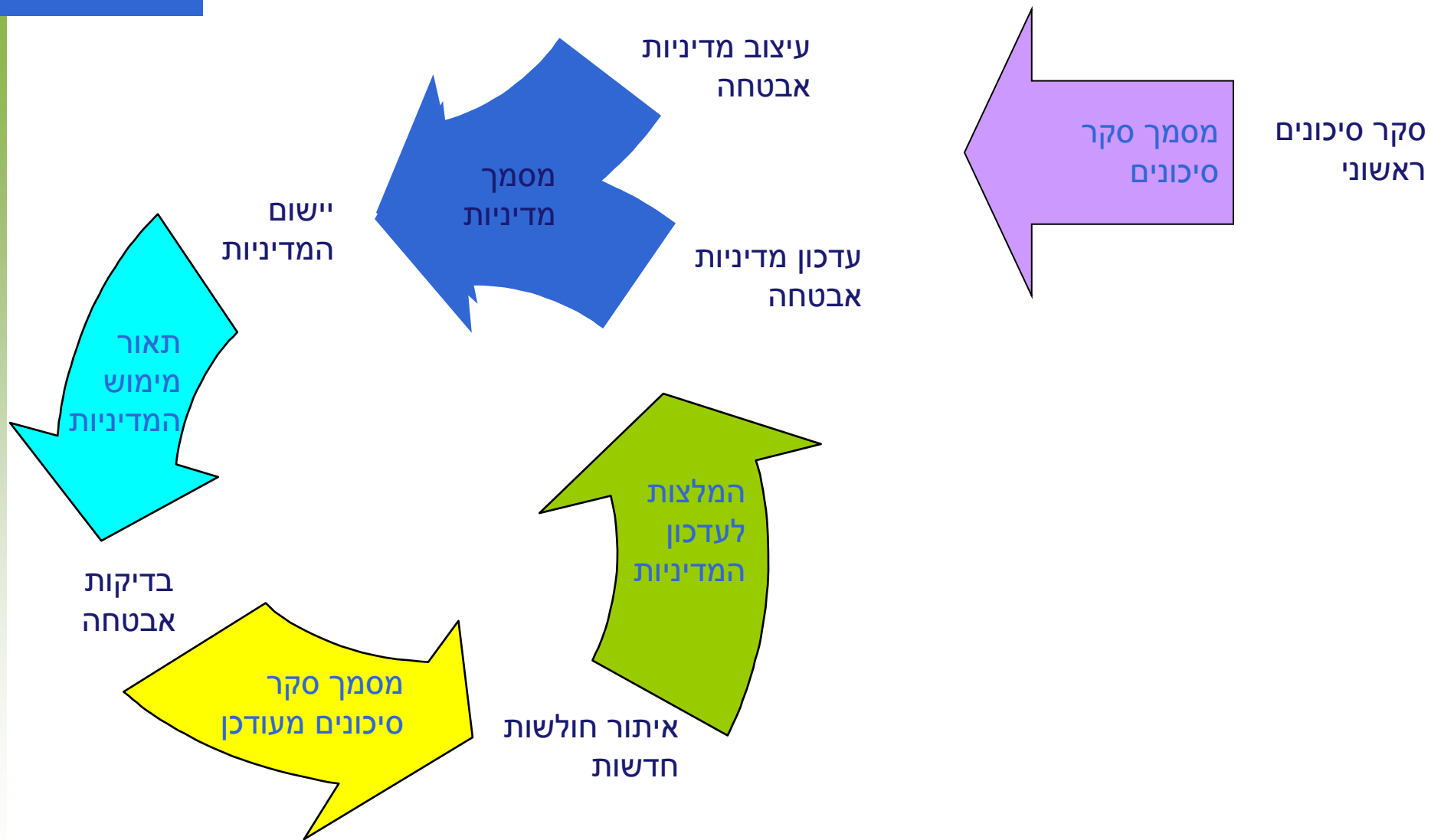
- פגיעה ברמת הביטחון
- חשיפת סודות צבא או מדינה
- פגיעה פיסית באנשים

## ❖ בתשתיות לאומיות

- הפסקת שירותים בסיסיים כגון חשמל, מים



# מודל אבטחת מידע



# מחזור חיים של פרויקט - ייזום



❖ ה"לקוח" של הפרויקט \ מומחה היישום

○ הממונה על אבטחת המידע

○ אנשי תשתיות המחשוב

○ ההנהלה

○ המשתמשים במערכות המידע.

❖ צריך למנות "לקוח מוביל" (לרוב - הממונה על אבטחת המידע בארגון), שיאסוף דרישות, מגבלות וחלומות בנושא אבטחת מידע.



# מחזור חיים של פרויקט - אפיון

## ❖ דגש על הנושאים הבאים:

- סקר סיכונים למערכות המידע בארגון
- הגדרה או עדכון מדיניות אבטחת מידע ארגוני

## ❖ נושאים אחרים להדגשה:

- היבטי חוק ומנהל בתחום אבטחת מידע
- סקירה ומיפוי של אמצעי אבטחה קיימים בארגון
- סקירת כלים לאבטחת מידע הקיימים בשוק

# מחזור חיים של פרויקט – בקשה להצעות



❖ גורמים לשונות בין פרויקטים:

- תכולת הפרויקט
- המצאות אנשים מומחים בארגון
- רמת שיתוף גורמים חיצוניים בבעיות אבטחת מידע רגישות בארגון.

❖ יש ארגונים שיעדיפו לבצע גם את שלב האפיון כולו בעזרת גורם מומחה/יועץ, ואז תהיינה מספר בקשות להצעה.

# מחזור חיים של פרויקט - עיצוב ובנייה

- ❖ שרטוט מדויק של ארכיטקטורת הרשת על מרכיביה כולל בקרות טכניות שהוחלט ליישם.
- ❖ הקמת סביבת ניסוי לבקרות הטכניות.
- ❖ כתיבת נהלים והוראות עבודה טכניים עבור הבקרות והרכיבים החדשים ברשת.
- ❖ כתיבת נהלי אבטחת מידע ארגוניים הנובעים מהמדיניות המעודכנת.



# מחזור חיים של פרויקט - בדיקות מערכת

- ❖ בדיקת הטמעה של הבקורות הטכניות בארכיטקטורה החדשה ע"פ הנהלים הטכניים שנכתבו בשלב הקודם.
- ❖ קבלת משוב על היכולת לקיים את הנהלים בארגון מקבוצת משתמשים נבחרת



# מחזור חיים של פרויקט - התקנה והרצה



## ❖ ברמה הארגונית

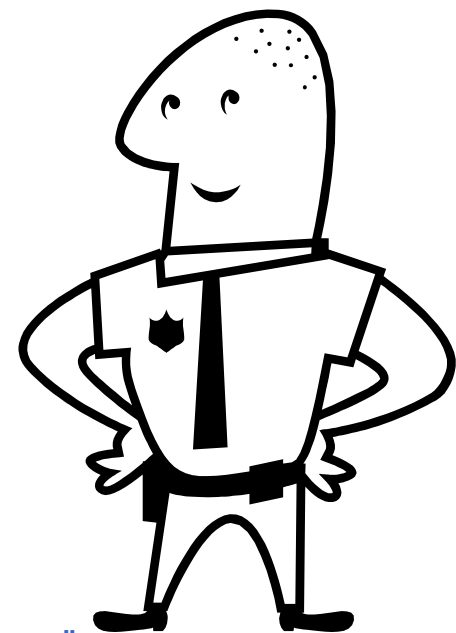
- מינוי אחראי לאבטחת מידע
- הטמעת מסמכי מדיניות ונהלים נגזרים
- הפעלת מנגנון לאכיפת המדיניות

## ❖ ברמה הטכנית

- הקשחת שרתים ורכיבי תקשורת
- אמצעי הגנה (Firewall, אנטייורוס, IDS)
- נהלים:
  - מימוש פתרונות האבטחה
  - נהלי "מקרים ותגובות" לאירועי אבטחת מידע
  - נהלי גיבוי ושחזור נהלי התאוששות מאסון

# מחזור חיים של פרויקט - תפעול ותחזוקה

- ❖ ביצוע מחזורי של בדיקות אבטחה וסקר סיכונים מעודכן, במטרה לאתר חולשות חדשות, טכניות וארגוניות.
- ❖ תוצר שלב זה - המלצות לעדכון מדיניות אבטחת המידע ברובד הטכני והארגוני.



# תוצרים בקיט

## ❖ תיק לפרויקט אבטחת מידע תשתיתי

- עץ מערכת מתמחה המדגיש היבטים ייחודיים לפרויקט

## ❖ מסמך סקר סיכונים

- מיפוי תהליכים ארגוניים
- מיפוי וניתוח מערכת
- מיפוי וניתוח אבטחה
- סיכום והמלצות

## ❖ מסמך מדיניות אבטחת מידע

- עקרונות אבטחת מידע כלליים
- מדיניות מפורטת



# מ תודה

