**נוהל אבטחת מידע בפיתוח מערכות, ארכיטקטורה, יישומים ושירותים**

גרסה: 2.0

סעיף בתקן: א.14.2.1

תאריך:

|  |  |  |  |
| --- | --- | --- | --- |
| פרטי השינוי | גרסה | נכתב על ידי | תאריך אישור בפורום אבט"מ |
| גרסה ראשונה | 1.0 |  | 19-05-2015 |
| עדכון בעלי תפקידים ואחריות | 2.0 |  | 29-03-2018 |
|  |  |  |  |
|  |  |  |  |
| נספחים: | | | |

# תוכן עניינים

[תוכן עניינים 2](#_Toc421012190)

[1. כללי.. 3](#_Toc421012191)

[2. מטרות 3](#_Toc421012192)

[3. הגדרות 3](#_Toc421012193)

[4. גוף הנוהל 3](#_Toc421012194)

[4.1. אבטחת מידע בסביבות פיתוח ובדיקות 3](#_Toc421012195)

[4.2. ארכיטקטורה מאובטחת 4](#_Toc421012196)

[4.3. שילוב אבטחת מידע בפיתוח 5](#_Toc421012197)

[4.4. אימוץ קוד פתוח 6](#_Toc421012198)

[4.5. שימוש בקבלן חיצוני לפיתוח יישומים 6](#_Toc421012199)

[5. בקרה 7](#_Toc421012200)

[6. מסמכים מתייחסים 7](#_Toc421012201)

# כללי

יישומים שנרכשו, יישומים בפיתוח עצמי, קוד מקור Open Source, מערכות, בסיסי נתונים ושירותים שונים, מהווים כולם חלק חיוני ממערכות המידע והמחשוב של חברה (להלן: "החברה").

בכל אחד ממרכיבים אלה, קיימים סיכוני אבטחת מידע העלולים להוביל לפגיעה בסודיות, שלמות, אמינות, זמינות ושרידות המידע ועל כן, הגדרת הנחיות עבודה ויישומן ההולם תוך שילוב אבטחת המידע, יאפשרו מזעור סיכוני האבטחה. כמו כן, הטמעתם של מרכיבים אלה באופן המאובטח ביותר דורש תכנון ארכיטקטורה שייקח בחשבון את מכלול הסיכונים השונים בכל רכיב ואת השפעתם המצטברת האפשרית האחד על השני וימזער אותם ככל הניתן.

# מטרות

* 1. הגדרת קווי יסוד לפיתוח יישומים באופן מאובטח, תוך שילוב היבטי אבטחת מידע בכל שלבי הפיתוח.
  2. הגדרת נוהל אחיד להטמעת יישומים, קוד מקור Open Source, מערכות, בסיסי נתונים ושירותים שונים באמצעות עקרונות של ארכיטקטורה מאובטחת.
  3. צמצום סיכוני אבטחת מידע פוטנציאליים, העלולים לנבוע משימוש בנתוני אמת בסביבות פיתוח ובדיקות.
  4. ניהול סביבת הפיתוח באופן שיבטיח שמירה ושלמות קוד המקור בכל שלבי הפיתוח.

# הגדרות

* 1. פיתוח מאובטח – שילוב היבטי אבטחת מידע בכל שלבי מחזור החיים של פיתוח תוכנה SDLC (Software Development Lifecycle).
  2. קוד מקור Open Source – קוד שמקורו ברשת האינטרנט הזמין לשימוש חופשי ע"י ארגונים ואשר מפותח ומתוחזק ע"י קהילת מפתחים שאינה שייכת בהכרח לארגון אחד.

# גוף הנוהל

## אבטחת מידע בסביבות פיתוח ובדיקות

### הגנה על המידע

1. ככל הניתן, עבור כל יישום המפותח בחברה תתקיימנה סביבות פיתוח ובדיקות, בנפרד מסביבת הייצור.
2. ככל הניתן, הגדרת הרשאות הגישה לסביבות פיתוח ובדיקות תהיה רק למפתחים ולאנשי היישום הנדרשים לבצע בהן בדיקות.
3. ככלל, לא יהיה מידע של לקוחות בסביבות פיתוח ובדיקות. במידה וקיים צורך עסקי לייבא מידע של לקוחות לסביבות אלה, המידע חייב להיות מעורבל באופן שלא יהיו בו פרטי עובדי לקוחות מזהים (ראו 'נוהל שימוש בהצפנה').
4. כל חריגה מהר"מ דורשת אישור מוקדם של מנהל אבטחת המידע.

### הגנה על קוד מקור

1. ככל הניתן, קוד המקור של יישומי חברה יישמר במערכות ייעודיות לכך, אשר מסוגלות להחיל הרשאות גישה ומידור בין פרויקטי פיתוח תכנה שונים. מתן הרשאות הגישה ובקרה עליהן הם באחריות מנהל הפיתוח הרלוונטי. באחריות מנהל הסיסטם הרלוונטי לוודא גיבוי יומי של קוד המקור השמור במערכות שבאחריותו.
2. במידה והקוד לא נשמר במערכת ייעודית, אין לשמור אותו על תחנות המפתחים ללא גיבוי יומי שלו על כונן רשת. יש ליידע את מנהל אבטחת המידע ולקבל את אישורו לדבר. באחריות מנהל הפיתוח הרלוונטי לוודא עם מנהל הסיסטם כי מבוצע גיבוי יומי של הקוד.

### העברת גרסה לייצור

1. ככל הניתן תתבצע הפרדת תפקידים בין האחראי לפיתוח הגרסה, לבין האחראי להעלות אותה לייצור. כל העברה של גרסה חדשה לייצור תעשה בהתאם לנוהל מסודר עבור אותו יישום. באחריות בעלי התפקיד לתעד את העברת הגרסה לייצור.
2. יישום המהווה תוכנת Client אשר מיועדת להתקנה במחשבי לקוחות, תעבור סריקת אנטי וירוס במערכת ההלבנה של החברה, על מנת לוודא כי אינה מכילה קוד עוין וכי לא תתקבל התראת שווא ממערכת אנטי וירוס של הלקוח. בדיקת היישום היא באחריות מנהל הפיתוח הרלוונטי, בשיתוף עם צוות הטכנאים.
3. במידה ונדרש אישור "מחמיר" להיעדר קוד עוין מיישום Client, יש לקבל את אישורו המוקדם של מנהל אבטחת המידע להעלות את הקובץ לבדיקה חיצונית באתר/ים שאושרו לכך (לדוגמה האתר Virus Total).
4. במידה ולקוח מבקש אישור מחברה על יישום שאינו נגוע, באחריות מנהל הפיתוח הרלוונטי לבצע MD5 Hash לקובץ, להפיק פלט מצולם של סריקה באתר החיצוני (בה רואים את אותו ה-Hash) ואת תוצאות הסריקה של הקובץ ולהעביר את ה-Hash, את הקובץ ואת פלט הסריקה לאישור הלקוח.
5. יישום חדש לחלוטין, מודול חדש ביישום קיים או יישום שעבר שדרוג גרסה משמעותי, לא יעלה לייצור בטרם עבר את אישור מנהל אבטחת המידע. במידה ובוצע שינוי משמעותי ברכיבים הנוגעים לאבטחת מידע (Login, מערכת הרשאות, הצפנה וכד'), יבוצע ליישום מבדק אבטחה ע"י גורם חיצוני, בהיקף שיקבע מנהל אבטחת המידע (לדוגמה סקר קוד Code Review, מבדק חוסן).
6. רק לאחר שגרסת היישום תהיה נקייה מחשיפות בחומרה בינונית ומעלה, ניתן יהיה להעלותה לייצור. תיקון חשיפות בחומרה נמוכה, יבוצע בהתאם ללו"ז שייקבע בין מנהל הפיתוח הרלוונטי ומנהל אבטחת המידע.

## ארכיטקטורה מאובטחת

בכל מצב של צורך בהטמעת יישומים חדשים או שינויים במיקומם של יישומים קיימים ברשת, יש לקבל את אישורם המוקדם של מנהל אבטחת המידע ומנהל הסיסטם הרלוונטי.

### חיבורים חיצוניים ליישום

1. יש לוודא כי לא תהיה גישה ישירה למידע ביישום מכל רשת חיצונית, לרבות רשת האינטרנט. מימוש הגישה ייעשה ככל הניתן תוך שימוש בארכיטקטורת 3-Tier. משמעות הדבר היא כי שרת האפליקציה שיהיה חשוף למשתמשים, לא ישמש גם כשרת בסיס הנתונים.
2. ככל הניתן יש לעשות שימוש ברכיבי אבטחת מידע אפליקטיביים בכל נקודה בה אמור להיות חיבור חיצוני של היישום לרשת האינטרנט או לרשתות חיצוניות אחרות. לדוגמה, עבור יישומי Web יש להשתמש לכל הפחות ברכיב WAF.
3. על יישומי חברה ללא יוצא מן הכלל, לתמוך בהצפנה באמצעות הצפנת תווך התקשורת (שימוש ב-TLS) ו/או בהצפנת המידע עצמו בהתאם לצורך (ראו 'נוהל שימוש בהצפנה'). עבור יישום שנוספת לו הצפנה חדשה ואמור להיות מיועד להתקנה אצל לקוח, נדרש אישור משותף של אגף היישום ואגף טכנולוגיות בטרם יופץ ללקוח.

### קליטת מידע בקבצים ליישום

1. בכל מקרה בו יישום משמש לקליטת מידע בקבצים מלקוח או מכל גורם חיצוני אחר שאושר לכך, יש להטמיע מנגנון לסריקת הקבצים מפני קוד עוין. המנגנון יופעל במערכת הנמצאת מחוץ לסביבה אליה אמורים הקבצים להיקלט. הפעלת הסקירה באחריות מנהל הסיסטם.
2. במידת האפשר והצורך, יש לבצע המרת פורמט של סוג הקובץ הנקלט על מנת למנוע חדירה של קוד עוין המוסתר למשל ב-Meta Data של הקובץ.
3. כל עוד לא נדרשת פעולת Upload מצד המשתמש, היישומים יפותחו באופן שיאפשר להם למשוך קבצים פנימה באופן חד כיווני, באמצעות רכיבים ייעודיים שימוקמו בסגמנט רשת ה-DMZ. הקבצים יגיעו לנקודת "חניה" בה יבדקו לגילוי קוד עוין או שיומרו לפורמט אחר, בטרם יימשכו פנימה לסביבת הייצור המאובטחת.

## שילוב אבטחת מידע בפיתוח

בכל מצב של צורך בפיתוח יישומים חדשים או שינויים ביישומים קיימים שיש להם נגיעה לאבטחת מידע, יש לשתף את מנהל אבטחת המידע בכל שלבי הפיתוח, החל משלב הייזום ועד לשלב העלייה לייצור. מנהל אבטחת המידע בשיתוף מנהל הפיתוח הרלוונטי, יקבעו אבני דרך בשלבי הפיתוח בהן יידרש אישור אבטחת מידע.

### שלבי הייזום והתכנון

1. באחריות מנהל אבטחת המידע לבצע הערכת סיכונים ולכתוב מסמך מענה אבטחת מידע. במסמך המענה תהיינה הנחיות רלוונטיות למפתחים. במידת הצורך ובהתאם למורכבות היישום, יוזמן יועץ אפליקטיבי מומחה לסיוע בגיבוש היבטי אבטחת המידע שיש לשלב ביישום.
2. מענה אבטחת המידע יועבר לאישור מנהל הפיתוח הרלוונטי.
3. באחריות מנהל הפיתוח להעביר את תוכן המסמך לאנשי הפיתוח.
4. מענה אבטחת המידע יהיה חלק בלתי נפרד מתיעוד הפרויקט.

### שלבי הפיתוח וה-QA

1. פיתוח יישומים בחברה יבוצע אך ורק באמצעות שפות פיתוח וכלי פיתוח שאושרו מראש ע"י מנהל אבטחת המידע. בתהליכי פיתוח יהיו מעורבים הגורמים הבאים:

* הנהלת החברה (באמצעות פורום אבטחת מידע): תשמש כגורם מאשר עבור שינויים מהותיים בשפות פיתוח ו/או כלי פיתוח.
* מנהל אבטחת המידע: ישמש כגורם מנחה למפתחים והוא הגורם האמון על עדכון מסמך מענה אבטחת המידע במידה וקיימות דרישות אבטחת מידע חדשות שלא קיבלו ביטוי במענה המקורי.
* מנהל הפיתוח: ישמש כגורם מנהל של כל שלבי הפיתוח. באחריותו לעדכן את מנהל אבטחת המידע בהתקדמות שילוב אבטחת המידע ביישום, כולל במידה ועולים צרכים חדשים שיש להתייחס אליהם גם בהיבטים של אבטחת מידע.
* מנהלי הסיסטם: יסייעו למפתחים בהטמעת היישום בשרתים וברשתות הרלוונטיים. באחריותם לעדכן את מנהל אבטחת המידע במידה ועולים צרכים חדשים מהפיתוח, אשר יש להם השלכות על מיקום התקנת היישומים או הדורשים שינוי בארכיטקטורת השרת/הרשת.

1. באחריות מנהלי הפיתוח בשיתוף מנהל אבטחת המידע, לאמץ כללים מקובלים בשוק לפיתוח מאובטח עבור שפת הפיתוח/הטכנולוגיה הרלוונטיים ליישום שתחת אחריותם. לדוגמה, בפיתוח יישומי Web ניתן לאמץ את מתודולוגיות OWASP. במידה ואימוץ כללים לפיתוח מאובטח אינו אפשרי, יש ליידע את מנהל אבטחת המידע בדבר ובאחריותו להנחות לגבי מימוש בקרות מפצות.
2. באחריות מנהלי הפיתוח לפעול למען הכשרת אנשי הפיתוח וה-QA בכתיבת קוד מאובטח ובאיתור פרצות בקוד (ראו 'תכנית הדרכת עובדים בהיבטי אבטחת מידע'). ההכשרה תהיה באופן שוטף ותתאם לטכנולוגיות שאושרו לשימוש בחברה.

### שלב העלייה לייצור

1. באחריות מנהל אבטחת המידע לתעד את היבטי אבטחת המידע בכל יישום ולעדכן את המסמך בהתאם לשינויים מהותיים בגרסאות היישום. כחלק מהמסמך, יבוצע תיעוד של:

* מיפוי המודולים והתהליכים המרכזיים ביישום.
* מיפוי המידע הרגיש וההצפנה שיושמה.
* התייחסות להיבטים של הגנת הפרטיות (במידה ורלוונטי).
* אמצעי האימות ליישום.
* מערך ההרשאות ביישום.
* ממשק ניהול היישום.
* בסיס הנתונים.
* כתיבת אירועים ל-Log ויצירת התראות במערכת ניטור אבטחת המידע.
* מיקום רכיבי היישום בארכיטקטורת הרשת.
* מיקום היישום בסביבות שאינן סביבות ייצור.
* עקרונות הפיתוח המאובטח שהנחו בפיתוח.
* קיומם של אמצעי הגנה אפליקטיביים הניתנים להגדרה בהתאם לבחירת הלקוח.
* אמצעי הגנה כלליים שהוטמעו ביישום.
* תיעוד כל מבדקי החוסן שבוצעו ליישום בשנתיים האחרונות.
* סיכוני אבטחת מידע שעדיין קיימים ביישום.

### טיפול בחשיפות אבטחה ביישום שנמצא בייצור

1. במידה וקיימים סיכוני אבטחת מידע ביישום שנמצא בייצור, מנהל הפיתוח הרלוונטי בשיתוף מנהל אבטחת המידע יגבשו תכנית לטיפול בסיכונים. סיכונים שיוריים יתועדו במסמך היבטי אבטחת המידע עבור היישום, כולל הסיבה לאי הטיפול בהם.
2. חשיפות אבטחת מידע שהתגלו ביישום בעקבות מבדק אבטחת מידע יתוקנו בהתאם ללו"ז משותף שיקבעו מנהל אבטחת המידע ומנהל הפיתוח.
3. חשיפות אבטחת מידע שהתגלו ע"י אנשי חברה או ע"י גורמים בצד הלקוח, יתוקנו בהקדם האפשרי. באחריות מנהל הפיתוח לקבל אישור לתיקון התוכנה במידה ויש לו נגיעה לאבטחת המידע, ממנהל אבטחת המידע. במידת הצורך בו קיימת דחיפות רבה, ניתן לקבל אישור טלפוני לדבר. באחריות מנהל הפיתוח בתיאום עם גורמי אגף היישום לתאם את הטיפול בחשיפות מול הלקוח.
4. באחריות מנהל הפיתוח לבדוק האם חשיפות אבטחה ביישום שהתגלו אצל לקוח, רלוונטיות גם ללקוחות אחרים ולתקנן בהתאם ללו"ז מסודר. בדיקה זו יש לבצע בסמוך ככל הניתן לגילוי החשיפה.
5. דיווח על החשיפה ביישום אצל הלקוח למנהל אבטחת המידע, לסמנכ"ל טכנולוגיות ולסמנכ"ל חברה, יהיה באחריות מנהל הפיתוח (ראו 'נוהל תגובה לאירועי אבטחת מידע').

## אימוץ קוד פתוח

1. שימוש בקוד פתוח שמקורו ברשת האינטרנט דורש אישור מוקדם של מנהל אבטחת המידע.
2. באחריותו לבדוק אם פורסמו חשיפות אבטחה (CVE) באמצעות אתרים מוכרים המנתחים סיכונים שונים ביישומים. רק במידה ולא התגלו בו חשיפות בחומרה גבוהה ובינונית, יאושר הקוד לשימוש בחברה.
3. במידה ונמצאו בקוד חשיפות גבוהות ובינוניות ואין מנוס משימוש בו, ניתן להשתמש בו אם הקוד יאומץ בחברה באופן מנותק מהגרסאות העתידיות שתופענה באינטרנט. תיקון החשיפות ע"י אנשי הפיתוח בחברה יוכנס לתכנית עבודה בהקדם האפשרי, טרם אישור לשימוש בקוד הפתוח.
4. טרם השימוש בקוד פתוח, באחריות מנהל הפיתוח הרלוונטי לוודא כי אין לקוד זכויות יוצרים המונעות מחברה להשתמש בו באופן הנדרש (ראו 'נוהל התאמה לדרישות החוק').

## שימוש בקבלן חיצוני לפיתוח יישומים

1. במידה ויוחלט להשתמש בקבלן חיצוני לפיתוח יישומים עבור חברה, באחריות מנהל הפיתוח האחראי על הקבלן ליידע את מנהל אבטחת המידע. מנהל אבטחת המידע יעביר הנחיות לגבי אופן הפיתוח ואופן מתן הגישה לעובדי הקבלן למתקני חברה.
2. על הקבלן לעמוד בחלק או בכל דרישות נוהל זה כפי שינחה מנהל אבטחת המידע. באחריות מנהל הפיתוח האחראי מטעם חברה לוודא כי הקבלן מבין את ההנחיות שיועברו אליו וכי הוא מבצע אותן הלכה למעשה.
3. באחריות מנהל הפיתוח האחראי לקבלן, ליידע את סמנכ"ל טכנולוגיות ואת מנהל אבטחת המידע בכל חריגה לא מתואמת של הקבלן מההנחיות שקיבל מחברה.
4. עבודת הקבלן שלא לפי הנחיות אבטחת המידע המקוריות, חייבת להיות מתואמת מראש ומאושרת ע"י מנהל אבטחת המידע, באחריות מנהל הפיתוח האחראי לקבלן.

# בקרה

1. מנהלי הפיתוח יבחנו פעם בשנה את ההרשאות של עובדיהם במערכת ניהול קוד המקור. באחריותם לשמור תיעוד של סקירת ההרשאות שבוצעה. הסקירה תישלח למנהל אבטחת המידע.
2. במידה וקיים חשש לפעולה חריגה במערכת ניהול הקוד, ייבדק קובץ הלוג (במידה וקיים) ויבוצע תחקיר ע"י מנהל הפיתוח הרלוונטי.
3. סקירה מלאה ועדכון של מסמך היבטי אבטחת המידע עבור כל יישום, תבוצע ע"י מנהל אבטחת המידע באופן שוטף בהתאם לצורך או, לפחות אחת לשנה בכדי לוודא כי המסמך מעודכן וכי סיכונים הקיימים ביישום מטופלים. סיכום הסקירה יועבר למנהל הפיתוח לאישור ותיעוד.

# מסמכים מתייחסים

* 1. תקן 27001, 14A.
  2. נוהל שימוש בהצפנה.
  3. תכנית הדרכת עובדים בהיבטי אבטחת מידע.
  4. נוהל תגובה לאירועי אבטחת מידע.
  5. נוהל התאמה לדרישות החוק.