0. <u>ניהול שינויים:</u>

תאריך	מחבר	גרסא	שינוי
1/3/07	רן אדלר	1.0	da
1/5/07	יהושע פסין	1.1	עריכה
16/2/08	יהושע פסין	1.2	שינוי שם מסמך ישים
9/8/09	מורנו נאור	1.3	מספור הנוהל בהתאם לתקן + הוספת סעיפים 5.6, 5.7.
19/02/2012	טליה זמיר יהושע פסין	1.4	התאמה לתקן ISO 27799
22/08/2012	טליה זמיר תמיר פלדמן	1.5	התאמה לתקן ISO 27799
30/09/2012	שי אמיר	1.6	אישור הנוהל

1. <u>מטרה</u>

קיום אבטחת התוכנה והמידע במערכות היישום.

2. <u>הגדרות:</u>

2.1. קלט/ פלט: תוצרי מערכת, תעבורת הנתונים במערכת.

3. <u>מסמכים ישימים:</u>

3.1. נוהל "פיתוח מערכות מאובטחות 7.9.2-א"

3.2. נוהל "א-12.1 "דרישות אבטחה מידע ברמת היישום"

3.3. נוהל "אבטחת תשתיות 7.9.2-ב"

4. <u>אחריות ליישום</u>

4.1. מנהלי פרויקטים.

4.2. מפעילי מערכות מחשוב.

4.3. מנהלת תחום פיתוח.

4.4. מנהל אבטחת מידע.

4.5. היועצת המשפטית.

5. <u>שיטה</u>

5.1. כללי

5.2. יש ליצור שלוש סביבות עבודה נפרדות לטובת פיתוח תוכנה. כל סביבה תוגבל לביצוע אחת מהפעולות הבאות: **(להרחבה בנושא פיתוח מאובטח יש לפנות לנוהל "פיתוח מערכות מאובטחות 7.9.2-א).**

א. פיתוח (Development).

ב. בדיקה (Test).

ג. ייצור – סביבת עבודה אמיתית (Production).

5.2.1. לכל סביבת עבודה יוגדר מנהל אחראי אשר יפקח על כל הפעילויות המתרחשות בסביבה.

5.3. תהליך פיתוח המערכת

5.3.1. בכל דרישה לפיתוח/ רכישה של מערכת מידע, ימלא המשתמש טופס בקשה ובו יסביר את דרישתו.

5.3.2. טופס הבקשה ייחתם ויאושר ע"י מנהל היחידה המבקשת ויועבר למנהל אבטחת מידע.

5.3.3. לכל מערכת מידע ימונה בעלים. באחריות בעלי מערכות מידע לקבוע את סיווג המערכת.

5.3.4. באחריות מנהל אבטחת המידע לקבוע את ההגנות הנדרשות ע"מ לשמור על רמה נאותה של אבטחת מידע בהתאם לרמת הסיווג של המערכת.

5.4. ניתוח וניסוח של דרישות אבטחה

5.4.1. בקרות המשתלבות בשלב תכנון מערכת הינן זולות משמעותית ליישום ותחזוקה מִבַּקרות המוספות מאוחר יותר.

5.4.2. בשלב ניתוח וגיבוש הדרישות של פיתוח מערכות חדשות או שיפור מערכות קיימות, מנהל אבטחת המידע יהיה מעורב ויזוהו כל דרישות האבטחה, ינומקו, יוסכמו ויתועדו כחלק מתיק איפיון המערכת.

5.4.3. דרישות האבטחה יביאו בחשבון את הבקרות האוטומטיות אשר יש לשלב במערכת.

5.4.4. דרישות האבטחה ואמצעי הבקרה ישקפו את הסיווג של הנכסים המעורבים, ואת הנזק הצפוי במקרה של כשל אבטחה או העדר אבטחה ולכן יש לקבוע את הדרישות רק לאחר שלב סווג והערכת הנכס על ידי בעלי המידע של הנכסים המעורבים בהתאם לנוהל הערכת סיכונים.

5.5. הדרישות לאבטחת מידע בהם יש להתחשב מופיעים בנוהל א-12.1 "דרישות אבטחה במערכות מידע" ובנוהל "אבטחת תשתיות 7.9.2-ב". בהיבט הפיתוח יש לפנות "פיתוח מערכות מאובטחות 7.9.2-א"

5.6. הרשאות גישה

5.6.1. הגישה לסביבת הפיתוח תותר למנהל הפרוייקט ולמנהל הפיתוח בלבד.

5.6.2. מנהל פרויקט הינו הגורם היחיד אשר לו הרשאות להעלות שינויים לייצור.

5.6.3. במקרה של כשל בייצור, מפתח/ים יקבל/ו הרשאה נקודתית לגשת לסביבת הייצור לצורך בדיקת הכשל. הגישה לסביבת הייצור תבוטל מיד עם תום הטיפול בכשל. יש להימנע ככל האפשר מביצוע שינויים ישירות בסביבת הייצור גם במקרה של כשל.

5.6.4. סביבת הבדיקה (Test), תשמש את המפתחים והמשתמשים לצורך ביצוע בדיקות קבלה לפני מעבר לייצור.

5.7. מעבר מפיתוח לייצור

5.7.1. באחריות מנהל הפרויקט לקבוע סט בדיקות לביצוע לפני העברה לייצור.

5.7.2. המעבר של מערכת מפיתוח לייצור יבוצע ע״י מנהל הפרוייקט בלבד. למפתחים לא יינתנו הרשאות הנדרשות לטובת ביצוע המעבר.

5.7.3. כל התקנת מערכת בסביבת הייצור תיעשה בתאום ובאישור של מנהל מערכות מידע.

5.8. הגבלות שינויים

5.8.1. בעת מסירת תוכנות לביצוע שינויים הן אצל ספק חיצוני והן בתוך הארגון, תוצף דרישה לביצוע שינויים ברמה המינימאלית ביותר האפשרית שתאפשר:

5.8.1.1. שדרוג התוכנה כנדרש להמשך תפקודה בצורה היעילה ביותר.

5.8.1.2. מניעת התנגשויות בין תוכנה בפיתוח לבין תוכנות או מערכות המוטמעות בארגון.

5.9. דליפת מידע

5.9.1.הרשאות גישה

5.9.1.1. הגישה אל סביבת הפיתוח תותר למפתחים, למנהלי הפרוייקט ולמנהל התשתיות בלבד.

5.9.1.2. הרשאות הגישה למפתחים תינתן בהתאם לשיוך פרוייקטלי. לכל פרוייקט תוגדר סביבת עבודה ייחודית כך שגישת המפתח תתאפשר לפרוייקטים אליהם הוא משויך בלבד.

5.9.1.3. סביבת הבדיקה (Test), תשמש את המפתחים והמשתמשים לצורך ביצוע בדיקות קבלה לפני מעבר לייצור.

5.9.2.מעבר מפיתוח לייצור

5.9.2.1. באחריות מנהל הפרויקט לקבוע סט בדיקות לביצוע לפני העברה לייצור (עפ״י עקרונות סעיף 5.5).

5.9.2.2. המעבר של מערכת מפיתוח לייצור יבוצע ע״י מנהל הפרוייקט בלבד. לא יינתנו ההרשאות הנדרשות לטובת ביצוע המעבר, למפתחים.

5.9.2.3. כל התקנת מערכת בסביבת הייצור תעשה בתאום ובאישור של מנהל התשתיות והתקשורת.

5.10. עקרונות מנחים לביצוע בדיקות קבלה

5.10.1. במהלך בדיקת ההטמעה של המערכת (Integration) יש לוודא כי אין למפתחים גישה למטרות עדכון וכי לא ניתן לבצע שינויים בקוד הנבדק ללא אישור.

5.10.2. אין להשתמש בהעתק של נתונים אמיתיים מסביבת הייצור (Production).

5.10.3. יש לתעד את נהלי הבדיקה כיאות.

5.10.4. בעת זיהוי בעיות במהלך הבדיקה, על המפתח לתעד את הבעיות, לבצע שינויים מתאימים בסביבת הפיתוח ולהגיש אותה לבדיקה חוזרת.

5.11. פיתוח תוכנה על ידי קבלני שירות

במידה ומוציאים את פיתוח התוכנה לגורמים מחוץ למשרד, יש לשקול את הנושאים הבאים:

5.11.1. סידורי רישוי, הבעלות על הקוד, וזכויות קניין אינטלקטואלי.

5.11.2. אישור האיכות והדיוק של העבודה המתבצעת.

5.11.3. סידורי הפקדה למקרה כשל של צד שלישי כגון פשיטת רגל, אבדן הקוד וכו׳.

5.11.4. זכויות גישה לבדיקת האיכות והדיוק של העבודה שנעשתה.

5.11.5. דרישות חוזיות לשילוב אבטחת מידע בקוד.

5.11.6. בדיקה לפני ההתקנה לגילוי קוד זדוני.

5.11.7. שימוש בתכנה אינו מצריך הרשאות מנהל (Administrator) בתחנה אלא של משתמש רגיל בלבד.

5.12. תחזוקת מערכות

5.12.1. נוהלי בקרת שינויים

יבוצעו הפעולות הבאות:

5.12.1.1. מילוי טופס "בקשה לאישור שינוי באפליקציה ובתשתיות מערכת" על ידי בעל מערכת המידע.

5.12.1.2. בעל מערכת המידע יגיש את הבקשה לשינוי למנהל הפרויקט, שיבדוק היתכנות השינוי.

5.12.1.3. במידה והשינוי בר ביצוע, מנהל הפרויקט יעביר את הבקשה למנהל הפיתוח ולמנהל אבטחת מידע.

5.12.1.4. במקרה שהבקשה כרוכה בשינוי המשפיע על יישום אחר, דרוש גם אישורו של בעל מערכת המידע של אותו יישום.

5.12.1.5. תבוצע סקירה של הבקרות הקיימות כדי להבטיח שהן לא יועמדו בסכנה על ידי השינויים.

5.12.1.6. זיהוי היישומים והתשתיות הדורשים שינוי בעקבות הבקשה לשינוי.

5.12.1.7. וידוא כי תיעוד המערכת מעודכן עם השלמתו של כל שינוי.

5.12.1.8. יבוצע ניהול גרסאות לכל עדכוני התוכנה.

5.12.1.9. תחזוקת נתיב ביקורת של כל הבקשות לשינוי.

5.12.1.10. וידוא כי תיעוד התפעול ונהלי המשתמש עודכנו במידת הצורך.

5.12.1.11. וידוא כי יישום השינוי מתבצע באופן הממזער הפרעות למהלך העבודה התקני.

5.12.1.12. וידוא כי יישום השינוי מתבצע באופן הממזער הפרעות למהלך העבודה התקיני בארגון בכלל וביחידה בפרט.

5.12.1.13. יש לבצע בדיקות אבטחת מידע לאחר השינויים.

5.12.2. דרישות שמירת התיעוד

מנהל מערכת המידע ישמור את כל טפסי בקשות השינוי, תוכניות הבדיקה לשינוי בתוכנית ותוצאות הבדיקות.

5.12.3. התקנת תוכנה (deployment)

תוכנה חדשה או תוכנה אשר עברה שינויים חייבת להיבדק כיאות ולקבל אישור בהתאם לסטנדרטים הארגוניים של ניהול שינויים ובעיות טרם התקנתה בסביבת הייצור של הארגון.

5.12.4. הגבלות שינויים לחבילות תוכנה

5.12.4.1. רצוי להשתמש בתכנות מדף מבלי לשנותן. כאשר נראה שיש צורך חיוני בשינוי בתכנה כזו, יישקלו הנושאים הבאים :

5.12.4.1.1. הסיכון לבקרות הדיוק והשלמות המובנים.

5.12.4.1.2. קבלת הסכמה בכתב מהספק המאשרת את ביצוע השינוי.

5.12.4.1.3. האפשרות לקבל את השינויים הדרושים מהספק, כעדכון תוכנה תקני.

5.12.4.1.4. ההשלכות הנובעות מכך שהארגון הופך להיות האחראי להמשך התחזוקה, עקב השינויים שהוכנסו.

5.12.4.2. שינויים יבוצעו על עותק של התכנה ולא על המקור. התכנה המקורית תשמר.

5.12.4.3. כל השינויים ייבדקו בדיקה מלאה ויתועדו כך שניתן יהיה, בעת הצורך, ליישם אותם שוב פעם בעתיד.

5.12.4.4. יש לבדוק שאין פגיעה באבטחת המידע לאחר השינוי.

6. חתימה

מנהל אבטחת המידע הינו הבעלים של מסמך זה והינו האחראי לוודא כי הנוהל תואם את הדרישות המובאות במנא"מ.
הנוהל אושר ונחתם בחתימה דיגיטאלית על ידי מנהל אבטחת המידע של משרד הבריאות או בא כוחו ומוגדר כנוהל רשמי של משרד הבריאות.