משרד הבריאות – נהלי אבטחת מידע			
פרק	**רכישה פיתוח ותחזוקת מערכות**	מהדורה	**2.0**
שם הנוהל	**אבטחה בתהליכי פיתוח, תמיכה ותחזוקת מערכות**	בתוקף מ	**ספטמבר 2015**
מספר	**14.2**		**עמוד 1 מתוך 7**

0. ניהול שינויים:

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
17/11/2014	אורנסק	1.7	התאמות לדרישות תקן ISO 27001:2013 עדכון סעיף 5.7.1
09/09/2015	גבי פטליס	1.8	בקרה
09/09/2015	שי אמיר	2.0	אישור

משרד הבריאות – נהלי אבטחת מידע			
פרק	**רכישה פיתוח ותחזוקת מערכות**	מהדורה	**2.0**
שם הנוהל	**אבטחה בתהליכי פיתוח, תמיכה ותחזוקת מערכות**	בתוקף מ	**ספטמבר 2015**
מספר	**14.2**		**עמוד 2 מתוך 7**

1. מטרה

קיום אבטחת התוכנה והמידע במערכות היישום בפיתוח של מערכת חדשה, רכישה של מוצר מדף ותחזוקה שוטפת של מערכות מידע וממשקים יעודיים.

2. הגדרות:

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

3. מסמכים ישימים:

3.1. נוהל **א-14.2.1 פיתוח מערכות מאובטחות**

3.2. נוהל **א-13.1 אבטחת תשתיות**

3.3. בנוהל **א-14.1.1 דרישות אבטחת מידע**

4. אחריות ליישום

4.1. מנהלי פרויקטים.

4.2. מנהלת תחום פיתוח.

4.3. מנהל אבטחת מידע.

5. שיטה

5.1. כללי

5.2. יש ליצור שלוש סביבות עבודה נפרדות. כל סביבה תוגבל לביצוע אחת מהפעולות הבאות:
להרחבה בנושא פיתוח מאובטח יש לפנות לנוהל א-14.2.1 פיתוח מערכות מאובטחות.

א. פיתוח (Development).

ב. בדיקה (Test).

ג. ייצור – סביבת עבודה אמתית (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 או רכישה של מערכת מידע יש לערב את גורמי אבטחת מידע לשם הבהרת מדיניות אבטחת המידע.

5.3.2. לכל מערכת מידע ימונה מנהל פרויקט לקבוע יחד עם המחלקה המשפטית את רמת הסיווג של המערכת.

5.3.3. באחריות מנהל אבטחת המידע לקבוע את ההגנות הנדרשות לאבטחת מידע בהתאם לרמת הסיווג של המערכת.

5.4. ניתוח וניסוח של דרישות אבטחה

5.4.1. 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 אפיון המערכת.

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

5.4.3. 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 להערכת הסיכונים.

5.5. הדרישות לאבטחת מידע בהם יש להתחשב מופיעים בנוהל **א-14.1.1 דרישות אבטחת מידע ברמת היישום** ובנוהל **א-13.1 נוהל אבטחת תשתיות**. בהיבט הפיתוח יש לפנות ל **נוהל א-14.2.1 נוהל פיתוח מערכות מאובטחות**.

5.6. הרשאות גישה

5.6.1. הגישה לסביבת הפיתוח תותר למנהל הפרויקט, למנהל הפיתוח והמפתחים בלבד.

5.6.2. מנהל פרויקט ינחה את הפיתוח בתהליך ביצוע השינויים ועליה לסביבת ייצור.

5.6.3. במקרה של כשל מערכת בסביבת הייצור, המפתחים יקבלו הרשאה ספציפית למקרה 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 QA ובדיקות אבטחה לביצוע לפני העברה לייצור. במסגרת הבדיקות ייבדקו רכיבי ומנגנוני אבטחת מידע שמופעלים במסגרת הפרויקט.

5.7.2. המעבר של מערכת מפיתוח לייצור יבוצע בהנחיית מנהל הפרויקט. למפתחים יינתנו הרשאות נדרשות לטובת ביצוע המעבר. ההרשאות יבוטלו עם תום המעבר.

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

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 הפרויקט ולמנהל התשתיות בלבד.

5.9.1.2. הרשאות הגישה למפתחים תינתן בהתאם לשיוך פרויקטלי. לכל פרויקט תוגדר סביבת עבודה ייחודית כך שגישת המפתח תתאפשר לפרויקטים 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 הפרויקט 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 אמתיים 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 ו פיתוח התוכנה מתבצע על ידי גורם חוץ 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. תיעוד הבקשה לאישור שינוי באפליקציה ובתשתיות מערכת.

5.12.1.2. יש לבחון היבטים לשינוי בממשקים עם מערכות מקבילות בארגון.

5.12.1.3. מיפוי הסיכונים ומתן פתרונות מתאמים על פי הצורך לשינוי.

5.12.1.4. זיהוי היישומים והתשתיות הדורשים שינוי בעקבות הבקשה לשינוי.

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

5.12.1.6. יבוצע ניהול גרסאות לכל עדכוני התוכנה.

5.12.1.7. תחזוקת נתיב ביקורת של כל הבקשות לשינוי.

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

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

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

5.12.1.11. יש לבצע בדיקות אבטחת מידע לאחר השינויים.

5.12.1.12. כל הבקשות לשינוי, בין אם התקבלו או נדחו, יתועדו במלואן ויהיו נגישות למנהל אבטחת המידע.

5.12.2. 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.

5.12.3. הגבלות שינויים לחבילות תוכנה

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

5.12.3.1.1. הסיכון לבקרות הדיוק והשלמות המובנים.

5.12.3.1.2. במידת הצורך, קבלת הסכמה בכתב מהספק המאשרת את ביצוע השינוי.

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

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

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

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

5.12.3.4. יש לבדוק שאין פגיעה באבטחת המידע לאחר השינוי.

6. <u>חתימה</u>

מנהל אבטחת המידע הינו הבעלים של מסמך זה והינו האחראי לוודא כי הנוהל תואם את הדרישות המובאות במנא"מ.