

 <p>מיאהקום انحاد قرى الجليل الأسفل للمياه والصرف الصحي م.ض תאגיד המים והביוב כפרי גליל תחתון בע"מ كفر كنا، طرعان، دبورية، المشهد، شبلي أم الغنم، البعينة - نجيدات، عين ماهل كفر كنا، טורעאן, דבוריה, משהד, שיבלי - אום אלגנם, בועינה - נוג'ידאת, עין מאהל</p>		תגובה לאירוע	
		אבטחת מידע	
		מהדורה: 1.0	מס' נוהל: א.16
תפקיד: יועץ חיצוני		עודכן בתאריך: 30/6/2018	
תפקיד: מנכ"ל התאגיד		ערך: טל רוזנשטיין	עמוד 1 מתוך 6
		אישר: סלאח נסאר	

1. ניהול שינויים:

שינוי	גרסא	מחבר	תאריך

2. מטרה

2.1 קביעת אחריות וסמכויות בניהול תקריות ואירועים וכן קביעת תהליכי הדיווח, הטיפול, התיעוד והפקת הלקחים מאירועי אבטחת מידע.

3. מסמכים ישימים

אין

4. אחריות ליישום

4.1 ממונה אבטחת מידע.

4.2 צוות מח' המחשוב.

4.3 מנהלים בתאגיד.

4.4 עובדי התאגיד

5. שיטה

 <p>انحداد قرى الجليل الاسفل للمياه والصرف الصحي م.ض תאגיד המים והביוב כפרי גליל תחתון בע"מ كفر كنا، طرعان، دبوریه، المشهد، شبلي أم الغنم، البعینة - نجيدات، عين ماهر كفر كنا، טורעאן, דבוריה, משהד, שיבלי - אום אלגנם, בועינה - נוג'ידאת, עין מאהל</p>		תגובה לאירוע אבטחת מידע	
		מס' נוהל: א.16	מהדורה: 1.0
עודכן בתאריך: 30/6/2018		עמוד 2 מתוך 6	
תפקיד: יועץ חיצוני	ערך: טל רוזנשטיין		
תפקיד: מנכ"ל התאגיד	אישר: סלאח נסאר		

5.1. אחריות לטיפול באירועים

5.1.1. מיד עם היוודע על אירוע אבטחת מידע, ממונה אבטחת מידע יבצע תחקיר ראשוני על מנת לוודא האם אכן מדובר באירוע אבטחת מידע ומה רמת החומרה של התקרית.

5.2. טיפול בתקריות אבטחה

5.2.1. תקריות אבטחה יחקרו על ידי ממונה אבטחת מידע בארגון על מנת לקבוע:

5.2.1.1. האם מדובר במערכת מצילת חיים או מערכת המכילה מידע חסוי.

5.2.1.2. האם מדובר בחשיפה / שינוי / שיבוש / הוצאת מידע חסוי .

5.2.1.3. מהי חומרת הנזק .

5.2.1.4. מהי סיבת התקרית.

5.2.1.5. מהי התגובה ההולמת לטיפול מידי.

5.2.1.6. מהי התגובה ההולמת לטיפול לטווח ארוך (פעולה מתקנת ומונעת).

5.2.1.7. כל עוד לא ידוע אחרת, קיים צורך להתייחס לאירוע כאל אירוע אשר עלול

להתפשט לכלל הרשת. על כן יש צורך בתגובה מהירה וחד משמעית.

5.2.2. בעת הצורך יש לזמן את היועצים חיצוניים אשר יעזרו להגדיר את האירוע ואת אופי התגובה לאירוע.

5.2.3. במקרה של אירוע ברשת, כל עוד לא ידוע אחרת, יש צורך להתייחס לאירוע כאל אירוע אשר עלול להתפשט לכלל הרשת. על כן יש צורך בתגובה מהירה וחד משמעית.

5.2.4. יש לפעול על מנת להבטיח את שלמות הראיות והאפשרות לנקוט בצעדים משפטיים אם המקרה מצריך זאת.

5.2.5. חברי ועדת ההיגוי לאבטחת מידע הנם הנציגים היחידים של התאגיד שישלימו את הפניית ההליכים הפליליים אל רשויות אכיפת או הסדרת החוק בעת הצורך.

5.2.6. כדי להבטיח הפקת לקחים מאירועי אבטחת מידע, יהיה מנגנון שיאפשר כימות וניטור של סוגי תקריות אבטחת המידע.

5.2.7. בעת הגדרת אירוע כאירוע בעל רמת סיכון גבוהה, ישולב נציג ועדת היגוי לאבטחת מידע/נציג הנהלה בכירה, כבר בתחילת הטיפול. על נציג זה מוטל:

 <p>מיאהקום انحاد قرى الجليل الاسفل للمياه والصرف الصحي م.ض תאגיד המים והביוב כפרי גליל תחתון בע"מ كفر كنا، طرعان، دبوريه، المشهد، شبلي أم الغنم، البعنه - نجيدات، عين ماهر كفر كنا، טורעאן, דבוריה, משהד, שיבלי - אום אלגנם, בועינה - נוג'ידאת, עין מאהל</p>		תגובה לאירוע	
		אבטחת מידע	
		מס' נוהל: א.16	מהדורה: 1.0
תפקיד: יועץ חיצוני		עודכן בתאריך: 30/6/2018	
ערך: טל רוזנשטיין		עמוד 3 מתוך 6	
תפקיד: מנכ"ל התאגיד		אישר: סלאח נסאר	

(1) לספק את תמיכת והנחיית ההנהלה למאמצי התגובה.

(2) להפנות או לאשר מימון.

(3) לקבוע את השלב שבו יש ליצור קשר עם גורמי אכיפת החוק.

(4) לדווח על התקרית לשאר חברי ההנהלה.

א. בכל צוות תגובה לתקרית מחשבים יהיה חבר צוות דלפק התמיכה אשר תפקידו לתעד

את התקרית ואת האמצעים שנקטו לצמצומה. באחריות הגורם המתעד לרשום, לתעד

ולארגן מידע מהתקרית כולל:

(1) פעולות החדירה.

(2) פעולות התגובה.

(3) תיעוד הזמן שהוקדש לחקירה (ניתן כך לחשב הפסד בגין שעות עבודה עבור כל

התקריות).

(4) תיאום איסוף רישומי מערכת, רשומות וכו' עם האחראי על איסוף הראיות.

(5) שמירת דוחות מרכזים של כל התקריות למטרת תיעוד היסטורי.

5.2.8. תקריות שאינן דחופות

(6) תקריות שאינן דחופות הן הפרות של מדיניות אבטחת המידע של התאגיד ושאין

כרוכות בסיכון אקטיבי של משאבי או מערכות התאגיד.

(7) באחריות צוות אבטחת המידע של התאגיד לטפל באירועים אלה כגון: שימוש לא

נאות במשאבי המערכת, התנהגות לא נאותה של עובד וכד'.

(8) צוות אבטחת המידע יסייע בחקירת אירועי אבטחת מידע, באיסוף ראיות

אלקטרוניות ו/או בתהליכי חקירה טכניים.

(9) במקרים אלו יבוצע הטיפול באופן נקודתי.

5.3. דיווח על אירועי אבטחה

5.3.1. כל אירוע או חשד לאירוע אבטחת מידע ידווח לממונה אבטחת המידע/נציג מח' המחשוב

בתאגיד. נציג זה ידווח מידית למנהל המחשוב בתאגיד.

 <p>מיאהקום انحاد قرى الجليل الاسفل للمياه والصرف الصحي م.ض תאגיד המים והביוב כפרי גליל תחתון בע"מ كفر كنا، طرعان، دبوریه، المشهد، شبلي أم الغنم، البعینة - نجيدات، عين ماهر كفر כנא, טורעאן, דבוריה, משהד, שיבלי - אום אלגנם, בועינה - נוג'ידאת, עין מאהל</p>		תגובה לאירוע	
		אבטחת מידע	
		מס' נוהל: א.16	מהדורה: 1.0
		עודכן בתאריך: 30/6/2018	
תפקיד: יועץ חיצוני	ערך: טל רוזנשטיין	עמוד 4 מתוך 6	
תפקיד: מנכ"ל התאגיד	אישר: סלאח נסאר		

5.3.2. משתמשים החושדים בפרצה או פגיעה באבטחת המידע כגון: פעילות חשודה בחשבונותיהם,

חשד לפגיעת קוד עיון (וירוס) במערכת כלשהי, השבתת חשבון, זמן התחברות (Login) אחרון יוצא דופן (במערכות המאפשרות זו), קבצים לא מוכרים, הודעות שגיאה לא מוכרות ממערכת המידע בה הם משתמשים או התנהגות חשודה אחרת - ידווחו על חשותיהם לממונה הישיר באופן מידי ובמקביל עליהם להעביר את הפרטים הנוגעים לתקרית אל נציג מח' המחשוב.

5.3.3. איש מח' המחשוב החושד בפרצה או פגיעה באבטחת המידע ידווח מיידית למנהל המחשוב אודות אירועי אבטחת מידע הכוללים תהליכים או יישומים חשודים, חיבורי רשת לא מוכרים, ניסיונות התחברות (Login) כושלים נשנים, חוסר עקביות בהתחברות (Login) או קבצים פגומים.

5.3.4. בכל מקרה של חשד לחשיפת מידע חסוי לגורמים לא מורשים (בתוך או מחוץ לתאגיד) יש לדווח למנהל הישיר והמנהל הישיר ידווח ל:

5.1.1.1. ממונה אבטחת מידע.

5.1.1.2. הנהלת התאגיד.

5.1.2. במקרה ועובד חושד שמתבצעת על ידי עובד אחר עבירה משמעתית או פלילית בנוגע לגילוי סודות או למסירת מידע שלא כדיון, עליו לדווח מיד לממונה על אבטחת המידע והממונה על המשמעת.

5.1.3. דיווח לגורמים חיצוניים נוספים כגון לקוחות וספקים או משטרת ישראל, ייעשה לפי להנחיות הנהלת התאגיד.

5.4. דיווח על נקודות תורפה

5.4.1. אם ידוע על קיומן של כשלים בנושא אבטחת המידע (אף אם טרם בשלו לכלל אירוע), ידווחו אלו למנהל/נאמן אבטחת מידע ולמח' המחשוב באופן מידי.

5.4.2. עובד לא יבצע בחינה של חולשות האבטחה ללא שיתוף ומעורבות של צוות המחשוב של הארגון.

5.5. טיפול בהתקפת וירוסים

 <p>מיאהקום انحاد قرى الجليل الأسفل للمياه والصرف الصحي م.ض תאגיד המים והביוב כפרי גליל תחתון בע"מ كفر كنا، طرعان، دبورية، المشهد، شبلي أم الغنم، البعنه - نجيدات، عين ماهل كفر كنا، טורעאן, דבוריה, משהד, שיבלי - אום אלגנם, בועינה - נוג'ידאת, עין מאהל</p>		תגובה לאירוע	
		אבטחת מידע	
		מהדורה: 1.0	מס' נוהל: א.16
תפקיד: יועץ חיצוני		עודכן בתאריך: 30/6/2018	
ערך: טל רוזנשטיין		עמוד 5 מתוך 6	
תפקיד: מנכ"ל התאגיד		אישר: סלאח נסאר	

5.5.1 אם יש חשד לוורוס במערכת כלשהי, על המשתמש לנתק מיד את המחשב מהרשת ולפתוח קריאה במח' המחשוב על אירוע אבטחת מידע. רק באישור מנהל המחשוב באתר יחובר המחשב אל הרשת מחדש.

5.5.2 צוות מח' המחשוב יפעל לאתר את מקור ההדבקה בוורוס ולבדוק האם נדבקו מחשבים נוספים בארגון על מנת להבטיח מתן מענה מלא לבעיה ומניעת הדבקה חוזרת ונשנית של מחשבים.

5.5.3 צוות מח' המחשוב ינהל את האירוע.

5.5.4 מנהל המחשוב ישקול אם לבודד את האתר הנפגע על מנת למנוע התפשטות הוורוס לאתרים נוספים בתאגיד.

5.6 תיעוד האירוע

5.6.1 כל אירוע אבטחת מידע יתועד וינוהל במח' המחשוב (מעבר לפתיחת הקריאה במערכת הקריאות) ע"ג "טופס תיעוד לפעולה מתקנת ומונעת (דפ"מ) – יזום" (ראה נספח א')

5.6.2 צוות מח' המחשוב יתעד את האירוע. תיעוד זה יתבצע באמצעות שמירת קבצים רלוונטיים, צילומי מסך וכד'.
 5.6.3 לאחר סיום האירוע מנהל הסיסטם יכתוב דו"ח המתעד את אירוע אבטחת המידע ואת הראיות שנאספו במהלכו ויעבירו למנהל אבטחת המידע.

5.7 הפקת לקחים מתקריות

5.7.1 אחת לרבעון ממונה אבטחת המידע יבצע ניתוח סטטיסטי אודות סוגי האירועים ומאפיינם בעזרת "טופס מעקב פעילות מתקנת ומונעת (דפ"מ)" (ראה נספח ב')

5.7.2 באחריות ממונה אבטחת המידע לקיים דיון להפקת לקחים במהלך התכנסות צוות אבטחת המידע.

5.7.3 במידה וממונה אבטחת המידע רואה לנכון, הוא יכנס את ועדת ההיגוי לאבטחת מידע, על מנת לדון באירוע ובהפקת הלקחים.

5.8 הליכי משמעת

 <p>מיאהקום انحاد قرى الجليل الاسفل للمياه والصرف الصحي م.ض תאגיד המים והביוב כפרי גליל תחתון בע"מ كفر كنا، طرعان، دبورية، المشهد، شبلي أم الغنم، البعينة - نجيدات، عين ماهر كفر كنا، טורעאן, דבוריה, משהד, שיבלי - אום אלגנם, בועינה - נוג'ידאת, עין מאהל</p>		תגובה לאירוע	
		אבטחת מידע	
		מהדורה: 1.0	מס' נוהל: א.16
תפקיד: יועץ חיצוני		עודכן בתאריך: 30/6/2018	
ערך: טל רוזנשטיין			
תפקיד: מנכ"ל התאגיד		אישר: סלאח נסאר	
		עמוד 6 מתוך 6	

- 5.8.1 פעולות משמעתיות כתוצאה מהפרה של מדיניות האבטחה ינקטו כנגד עובדים ו/או קבלנים ו/או ספקים ותהינה בהתאם לרמת החומרה של האירוע בהתאם לתוצאות החקירה.
- 5.8.2 פעולות משמעתיות יכולות לכלול בין היתר שלילת הרשאות גישה למקורות עיבוד מידע, פיטורין של יועצים, ביטולי חוזים, פיטורי עובדים וכדו'
- 5.8.3 צעדי המשמעת יינקטו בתיאום עם מנהל משאבי אנוש.

6. חתימה

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