נוהל מדיניות אבטחת מידע - אלטמן

תאריך	גרסה	שם
16 יולי 2019	גרסה 1	גיל פז

1. מטרת הנוהל

מטרת הנוהל להגדיר את מדיניות "אלטמן בריאות שותפות כללית" להלן **החברה** בתחום אבטחת המידע ואת פעילויות המחשוב למניעה, תחזוקה וניהול משימות אבטחת מידע.
תחום אבטחת מידע בארגון מרכז את המשימות שמבוצעות על מנת להבטיח שימוש ראוי במשאבי המחשוב של החברה, שמירה על אמינות המידע, שמירה על זמינותו, מניעת רוגלות, חדירות לא מורשות ווירוסים למיניהם, הדרכת המשתמשים לשימוש נכון ומאובטח בציוד המחשוב, המידע ואמצעי האחסון בחברה.

נוהל זה הינו בכפוף ואינו גורע מנוהל ל"הנחיות אבטחת מערכות המידע – מוצרי מעברות".
\\netapp\sharednew\Computer_Dep\ נהלים\נהלי אבטחת מידע ותקנות הגנת הפרטיות\הנחיות אבטחת מערכות המידע לעובדים 2018.docx

2. תיחום הנוהל

הנוהל מיועד לעובדי החברה, לספקי מערכות המחשוב וספקים נוספים בתחומי מערכות המידע גורם המחזיק במידע השייך לחברה. הנוהל מחייב כל גורם המטפל בשרתים ו/או בתחנות העבודה ו/או במאגרי המידע.
הנוהל מציג תיאור הפעולות שיש לבצע בתחום אבטחת מידע לרבות בתחום תשתית, ניהול הרשאות וסיסמאות, טיפול באירועים, הפצת מדיניות ומניעה.

3. תהליכי עבודה

להלן תהליכי עבודה הנכללים בנוהל:

4.1. התקנת תוכנות לא מאושרות.
4.2. התקנת תוכנות המורדות מהאינטרנט.
4.3. עדכוני תוכנה.
4.4. גלישה באינטרנט.
4.5. שימוש בדוא"ל.
4.6. טיפול בספאם.
4.7. אנטי וירוס.
4.8. ניהול סיסמאות.
4.9. אחסון מידע, ניהול משתמשים והרשאות.
4.10. מחשבים ניידים.

4. מדיניות בתחומי אבטחת המידע

4.1. התקנת תוכנות לא מאושרות

במחשבי החברה המשתמשים לא יוגדרו כמנהלים (Admin) של המחשב.
השימוש בתוכנה לא מאושרת עלול לגרום לשיבושים במערכות המחשוב של החברה.
התקנת תוכנה לא מאושרת תכלול בין היתר את הרכיבים הבאים:

1. תוכנה לא חוקית, תוכנה מועתקת ללא הרשאה או שנרכשה באופן אחר שלא בהתאם לתנאי הספק המורשה ולהנחיות החברה.
2. כל תוכנה אחרת, גם אם נרכשה כחוק ע״י העובד באופן פרטי, המותקנת ללא קבלת אישור מנהל מערכות המידע בחברה.

כל משתמשי תחנות עבודה שבמחשבם קיימת או שהותקנה תוכנה לא מאושרת מחויבים להודיע על כך. היה ועובד מצא שתוכנה לא מאושרת כלשהי הינה חיונית לעבודתו השוטפת עליו לפנות למנהל מערכות המידע על מנת לבצע הסרה, או שתבוצע רכישה באופן חוקי ע״י החברה, או שהתוכנה תקבל אישור התקנה ושימוש מן הגורמים המוסמכים.
האחריות לגבי השימוש בתוכנה לא מאושרת תהיה על המשתמש באופן אישי, גם כלפי החברה וגם כלפי גורמים חיצוניים.

4.2. התקנת תוכנות המורדות מהאינטרנט

התקנת תוכנות כאלה במחשבי החברה אסורה גם אם התוכנה מסוג Shareware או Freeware.

4.3. עדכוני תוכנה

1. כל המחשבים יוגדרו לבצע עדכון אוטומטי של מערכת ההפעלה כולל אתחול בסיום העדכון.
2. כל התוכנות יעודכנו לגרסאות המתקדמות ביותר שניתן.

4.4. שימוש בדוא"ל של החברה

שימוש בדואר אלקטרוני שלא לצורכי עבודה:
שרותי הדואר האלקטרוני הינם לצורכי עבודה בלבד. למניעת דלף מידע, אין להשתמש בשירותי הדואר האלקטרוני להעברת מידע שלא לצרכי העבודה. במקרים בהם נתקל עובד בחשד לשימוש שלא לפי הנחיות אלו עליו לדווח למנהלו.

קבלת דבר דואר מגורם לא ידוע:
במקרה בו משתמש מקבל דואר אלקטרוני עם צרופה מגורם לא ידוע, עליו למחוק את ההודעה כדי למנוע העברת וירוסים וסוסים טרויאניים לתוך מחשבי החברה.

4.5. גלישה באינטרנט

הגלישה באינטרנט תהיה מבוקרת על ידי מערכת לסינון אתרים מסוכנים ועם יכולת זיהוי וטיפול בתוכנות זדוניות.

4.6. טיפול בספאם

מערכת סינון דואר אלקטרוני מנטרת באופן רציף כל העברת מידע מהחברה ואליו בדואר אלקטרוני ומאתרת מידע מסוג ספאם ויכולה לחסום אותו.

על כל אירוע של ניסיון להעברת מידע שנחסם ע״י מערכת סינון דואר אלקטרוני, תיבדק סיבת החסימה, במקרה של חסימת שווא ישחרר הטכנאי את הדואר החסום.

4.7. אנטי וירוס

בכל גילוי וירוס בתחנת עבודה, מבוצעות פעולות לנטרל נזק ולמנוע התפשטות וירוס ברשת. בכל תחנת עבודה מותקנת תוכנת אנטי וירוס ברשת המנטרת את פעילות התחנה באופן שוטף. עם גילוי וירוס בתחנה, מציגה תוכנת האנטי ווירוס הודעה מתפרצת על המסך המיועדת ליידע את המשתמש. עם הופעת הודעה מתפרצת, המשתמש יודיע טלפונית מיד על גילוי ווירוס במחשבו לטכנאי השירות והתמיכה של החברה.

4.8. ניהול סיסמאות

אבטחת המידע ברשת מתבססת על זיהוי אמין של המשתמשים. סיסמאות הינן הכלי להגן על חדירה למערכות ולמחשבי הארגון, למידור, למניעת ריגול, למניעת גרימת נזק, ולמניעת חשיפת מידע למי שאינו מוסמך לכך.

1. על הסיסמאות להיות מורכבות ועליהן להשתנות אחת לתקופה כמוגדר להלן:
2. מחרוזת בת - 8 תווים לפחות המורכבת מאותיות, ספרות וסימנים לפי בחירת המשתמש.
3. משך זמן מרבי לתוקף סיסמת עבודה פרק הזמן המרבי שנקבע לשימוש בסיסמת עבודה הוא 3 חודשים ממועד יצירתה. כל פרק זמן נתון של 3 חודשים, המשתמש חייב לשנות את סיסמתו לחדשה שלא השתמש בה בעבר.
4. משתמש רשאי ויכול להחליף סיסמתו גם לפני שחלפו 3 חודשים ממועד יצירתה, אולם לא יותר מהחלפת סיסמא פעם אחת ביממה.
5. חשוב להבטיח כי המשתמשים אינם מתבססים על אותה סיסמא לכל השירותים שלהם.
6. סיסמאות הן אישיות וחל איסור לגלותן לאחר.

4.9. אחסון מידע, ניהול משתמשים והרשאות.

1. גישה לתיקיות ברשת תבצע על בסיס הרשאות כך שכל עובד יוכל לפתוח רק תיקיות וקבצים הדרושים לעבודתו לצורך מניעה של תוכנות כופר וגניבת מידע.
2. יוגדרו תיקיות רגישות בכל חברה, עם גישה מוגבלת לבעלי הרשאות בלבד ובהן ישמר המידע הרגיש.

4.10. מחשבים ניידים

1. המחשבים הניידים מיועדים להתחברות מרחוק בלבד, בעזרת סיסמה חד פעמית.
2. אין לשמור מידע על מחשבים ניידים.

5. נספח א: עקרונות מנחים באבטחת מידע לכלל החברות בקבוצה - בסיס מינימאלי

\\netapp\sharednew\Computer Dep\עקרונות הגנת הפרטיות\נהלים\נהלי אבטחת מידע ותקנות
docxמנחים באבטחת מידע לכלל החברות בקבוצה - בסיס מינימאלי הכרחי.