מועצת הצמחים

המועצה לייצור צמחים ולשיווקם

08 ינואר 2020
י"א טבת תש"פ

לכבוד

עו"ד אלעד מן
יועמ"ש הצלחה
דרך מנחם בגין, רמת גן 52681
רמת גן 52681

בדוא"ל

שלום רב,

הנדון: **בקשה חופש מידע – אמות מידה, נהלים והוראות לעניין פרטיות**

בהמשך לפנייתך שבנדון ;

1. פעם נוספת שהודעתך מתקבלת למחיצת ספאם ומשום כך העיכוב במענה.
2. מועצת הצמחים מחזיקה במאגרי המידע הבאים:
   - מאגר נתוני מגדלים ומשווקים של צמחים – מאגר רשום מס 600016768 מתאריך 23/12/2013
     מאגר זה משמש למעקב אחר נתוני גידול, שיווק וביצוע הדברות בקרב מגדלי פירות וירקות. למאגר יש פחות מעשרה מורשי גישה והוא עומד בתקנות הגנת הפרטיות (אבטחת מידע) תשע"ז -2017.
   - מאגר נתוני עובדי המועצה – בתהליך רישום.
     מאגר זה משמש לפעילות המועצה בלבד וכולל מידע לצרכי שכר ועומד גם הוא בתקנות הגנת הפרטיות.
3. מצורף נוהל אבטחת המידע של המועצה לפי תקנה 4 לתקנות הגנת הפרטיות (אבטחת מידע) תשע"ז – 2017.

בכבוד רב,

אביגיל לוי
הממונה על חופש המידע
המועצה לייצור צמחים ולשיווקם

דרך העצמאות 40 יהוד-מונוסון 5610102 ת.ד 235
Derech Ha'atzmaut 40 Yehud-Monosson
P.O.B 235 Yehud –Monosson ,5610102
WWW.PLANTS.ORG.IL

ענף הזית OLIVE DIVISION | ענף הירקות VEGETABLES DIVISION | ענף ההדרים CITRUS DIVISION | ענף הפירות FRUIT DIVISION

ניהול שינויים			
תאריך	מחבר	גרסה	שינוי

נוהל אבטחת מידע

1. מטרה :

מסמך זה מגדיר את מדיניות מועצת הצמחים בכל הקשור לאבטחת המידע, שימוש נאות במשאבי המחשוב השייכים לארגון ושמירה על הגנת הפרטיות. מטרת הנוהל הינה להגן ולשמור על נכסי המידע השייכים למועצה על פי עקרונות אבטחת המידע (שלמות המידע, סודיות המידע וזמינות המידע). מטרת הנוהל המרכזית הינה לצמצם את הסיכונים החיצוניים והפנימיים הכרוכים בעבודה בסביבה ממוחשבת בארגון, תוך כדי הצבת מסגרת כללים והעלאת מודעות העובדים לסיכונים השונים.

2. הוראות הנוהל

2.1. כללי

2.1.1. מועצת הצמחים אחראית לפרטיותם של הרשומים במאגרי המידע שלה. לא יעשה כל שימוש במידע פרטי ללא אישור מפורש מן האנשים או הגופים עליהם נשמר המידע.

2.1.2. הממונה על אבטחת המידע והגנת הפרטיות במועצה הינה: אביגיל

2.2. עובדי המועצה

2.2.1. בעת יציאה מן המשרד חובה לנעול את המחשב (מקש תלונות + L) ולנעול את המשרד .

2.2.2. העובדים רשאים לקחת עימם מחשבים ניידים והתקנים נשלפים עם מידע שאינו מסווג ו/או מאגרי מידע הכוללים מידע פרטי לטובת מצגות ,ישיבות ,כנסים , השלמת עבודה ,נסיעות לחו"ל וכו' .

2.2.3. העובדים ימנעו גישה אל מחשבם מכל מי שאינו מוסמך לכך .

2.2.4. כל עובד יקבל גישה בשרת לתיקיות הנוגעות לתחום עיסוקו בלבד ולתיקיות שיתוף ציבוריות עפ"י הצורך.

2.2.5. העובדים ישמרו מידע חשוב בתיקיות שבשרת ולא על גבי התחנות עצמן בהן לא מתבצע גיבוי .

2.2.6. העובדים אינם רשאים להביא מחשבים פרטיים ולחברם לרשת במקום העבודה.

2.2.7. העובדים ישמרו על סודיות המידע : חל איסור על הוצאת תומרי עבודה ו/או מאגרי נתונים הכוללים מידע פרטי ממחשבי הארגון ללא אישור מפורש מהממונה על אבטחת המידע.

2.2.8. **נוהל סיסמאות :** לכל עובד יוגדרו שם משתמש וסיסמה מורכבת (6-8 תווים של מספרים ,אותיות וסימנים) לטובת גישה למחשבו ומשם עפ"י הצורך לבסיס הנתונים שבשרת . הסיסמה תוחלף אחת לחצי שנה . אם קיים חשש לדליפת הסיסמה העובד יכול ורשאי להחליף את סיסמתו עוד קודם לכן .על העובד לזכור את סיסמתו ולא לרשום אותה במקום גלוי לאחרים .

2.2.9. **נוהל דואר אלקטרוני :** הדוא"ל הינו לשימוש צרכי עבודה בלבד ,יש לנקוט משנה זהירות במשלוח וקבלת הודעות דואר אלקטרוני. אין לשלוח הודעות שרשרת ולהפיץ הודעות תוך התחזות . אין לפתוח קבצים מצורפים מגורמים אשר אינם מוכרים או שהעובד איננו מצפה להם.

פרטיות הדואר מוגבלת – על העובד לדעת כי ניתן לגשת לדואר שלו בכל עת בהתאם לצרכי הארגון.

2.2.10. חל איסור על כל שימוש בתוכנות ללא רשיון ,תוכנות לא מורשות ,תוכנות שיתופיות והורדת תכנים שאינם חוקיים ברשת האינטרנט.

2.2.11. במקרה של אירוע אבטחת מידע – תוכנת האנטי וירוס תציג הודעה מתפרצת על המסך .במקרה כזה יש להקפיא את העבודה על המחשב ,לסגור את חיבורי הרשת ולעדכן את מנהל הרשת באופן מיידי .

2.2.12. בסיום יום העבודה על העובד לכבות את מחשבו האישי.

2.3. מנהל רשת

2.3.1. רישוי התוכנות ועדכונן השוטף – מערכות הפעלה ,אופיס ,אנטי-וירוס ,גיבוי וכו' – באחריות מנהל הרשת מול ספקי התוכנה הרלוונטיים ובאישור המנכ"ל.

2.3.2. על הרשת מגן רכיב FIREWALL שיעודכן מעת לעת בנוגע לאיומים חדשים .רק למנהל הרשת יש גישה לתוקי ה FIREWALL וליצירת חיבורים מרחוק בעת הצורך .

2.3.3. השרתים והתחנות מוגנים באמצעות תוכנת אנטי-וירוס . מנהל הרשת אחראי לביצוע תחזוקה שבועית של עדכוני תוכנה ,ניקוי רוגלות ובחינת תקינות תוכנת האנטי – וירוס.

2.3.4. מנהל הרשת יבצע ביקורת תקופתית של תחנות העבודה לבחינת החומר השמור בהן ,בדיקת מצב עדכוני המערכת ובדיקת הימצאותה של תוכנת האנטי-וירוס.

2.3.5. מנהל הרשת אחראי על כיבוי השרתים באופן מוסדר בימים בהם תתרחשנה הפסקות חשמל יזומות . (יקבל הודעה מראש ממזכירות הארגון)

2.3.6. מנהל הרשת אחראי לגריטה ולהשמדה של מחשבים ישנים עם החלפתם ולמחיקת כל התוכן מן הדיסקים הקשיחים שבהם.

2.4. ממונה אבטחת המידע והגנת הפרטיות

2.4.1. ממונה אבטחת המידע יעדכן את העובדים בסיכונים, איומים ,וירוסים ,תוכנות הצפנה וימים בהם צפויה מתקפה על אתרים.

2.4.2. במקרה של אירוע אבטחת מידע אחראי ממונה אבטחת המידע על תיאום בין מנהלי הרשת ועובדי המועצה.

2.4.3. במקרה של אירוע אבטחת מידע ממונה אבטחת המידע אחראי על תיעוד האירוע והודעה לגורמי האכיפה הנדרשים.

2.5. אמצעי הגנה פיזיים (חדר שרתים)

2.5.1. כל מחשב יחובר לאל-פסק במטרה להגן עליו מהפסקות חשמל פתאומיות ונחשולי מתח.

2.5.2. ציוד כיבוי אש (מטף תקין) ימצא באופן קבוע בהישג יד בחדר השרתים.

2.5.3. חדר השרתים מוגן בדלת פלדת כאשר המפתח נמצא אצל: מנהלת הרשת, מנהל 400AS ומנהל האחזקה.

2.5.4. הכניסה לחדר השרתים מצולמת ומנוטרת במצלמה במעגל סגור.

2.6. גיבוי

2.6.1. גיבוי מתבצע בענן – ע"י תוכנת ARCSERVE לשרתי חברת CCC.

2.6.2. פעמיים בשנה מתבצעת בדיקת שחזור למידע.

2.7. אחריות:

2.7.1. האחריות לפעול לפי הנהלים מוטלת על כלל עובדי המועצה . אכיפת הנהלים תהינה באחריות ממונה אבטחת המידע.