ירושלים,ט''ו בטבת התש''פ

12 ינואר ,2020

מס' תיק - 147/2019

לכבוד

עו"ד אלעד מן

דרך מנחם בגין 7

רמת גן

שלום רב,

הנדון: **אמות מידה, נהלים והוראות לעניין פרטיות**

שלום רב,

1. לבקשתך, מצורפים הנהלים, ההנחיות ואמות המידה של משרד האוצר בעניין מדיניות הפרטיות שלה בכל הנוגע לשמירה, טיפול, אחסון, הפצה, הנגשה, העברה וכו' של מידע ונתונים, הבאים:
2. נוהל הוועדה להעברת מידע של משרד האוצר.
3. נוהל ניהול משאבי הגנת המידע והסייבר.
4. נוהל ניהול סיכונים.
5. נוהל פעולה מתקנת והזדמנויות לשיפור.
6. נוהל טיפול במידע ובמצעי מידע.
7. נוהל סיווג המידע.
8. נוהל החלפת תפקיד.
9. פורמט הנחיות למנהל מאגר מידע במשרד האוצר.
10. פורמט הנחיות לנאמן אבטחת מידע במאגר מידע.
11. תעודה מטעם מכון התקנים הישראלי לפיה המשרד עומד בתקן ISO 27001.
12. בנוסף לנהלים המצורפים והמפורטים כאמור לעיל, קיימים במשרד האוצר נהלים נוספים אשר חשיפתם עלולה להעמיד את משרד האוצר בסיכון ממשי לפגיעה במאגרי המידע שלו, זאת משום שמנהלים אלה ניתן ללמוד על אמצעי אבטחת המידע הקיימים במשרד, אבטחת פיזית וסביבתית של המאגרים, הוראות לעניין גיבוי נתונים ועוד. כיוון שחשיפת נהלי אבטחת המידע אלה עלולה בוודאות קרובה לשבש את יכולתו של המשרד לנהל ולהחזיק את מאגרי המידע בתנאים הנדרשים, ובהתאם להוראת סעיף 9(ב)(1) לחוק חופש המידע, יצוינו שמות נהלים אלה ופירוט סוג ההוראות הקבועות בהם בלבד, כדלהלן:
13. **נוהל מבדקים פנימיים** – נוהל לבדיקת יישום ואכיפת מדיניות ובחינת התאמת המערכת והתשתית הטכנית, למדיניות ולנהלי הגנת המידע והסייבר של משרד האוצר.
14. **נוהל מדיניות הגנת המידע** – מבוסס על מדיניות אבטחת המידע המאושרת של המשרד (המדיניות מתווה את העקרונות המנחים והמהווים בסיס לנהלי העבודה בתחומי הגנת המידע והסייבר השונים במשרד) הנוהל נותן מענה אפקטיבי לסיכומי אבטחת המידע כפי שהוצפו בסקר סיכונים שבוצע במשרד על ידי מבקר חיצוני.
15. **אבטחת חדר המחשב** – הגדרת שיטות מידור ואבטחה פיזית של יחידת המחשב המרכזי והפונקציות התפעוליות הקשורות אליה.
16. **הגנה על המידע בתחנות קצה** – מטרת הנוהל היא להגדיר את הנחיות הגנת המידע והסייבר הקשורות לעמדת קצה בהיבטי אבטחה לוגית ואבטחה פיזית וכן שיטות ואמצעי אבטחה למשתמשי עמדת הקצה, למניעת דליפת מידע ממשלתי רגיש וכן למניעת האפשרות של חדירת גורמים לא מורשים לרשת המשרד.
17. **נוהל הפרדת סביבות עבודה** – מטרת הנוהל היא לייצר הפרדה בין סביבת הייצור לסביבת הפיתוח וסביבת הבדיקות, תוך צמצום נזקים פוטנציאליים העלולים לנבוע מעבודה בסביבה אחודה וחשיפת מידע לאינם מורשים.
18. **אבטחת מידע בקרב ממשקים עסקיים** - התוויית הטיפול, מבחינת הגנת המידע והסייבר, בפעילות הממשקים העסקיים והעובדים במשרד, במטרה להביא לתהליכים אופטימאליים המיושמים תחת עקרונות אחידים.
19. **אבטחת מידע במעבר לענן ציבורי** - כיצד יש לבצע הערכת סיכונים ולממש את הבקרות הנדרשות במעבר לסביבת ענן.
20. **נוהל אירועי אבטחת מידע** - מגדיר את תהליך העבודה של הגופים השונים במשרד, כאשר מתרחש אירוע המוגדר כאירוע הגנת סייבר. הנוהל מסדיר את הנושאים הבאים: הגדרת תהליכים לטיפול באירוע הגנת סייבר, מזעור וניטור נזקים הנובעים מאירועי הגנת סייבר, יצירת הליך להפקת לקחים למניעת הישנות מקרה דומה, הגדרת התהליך לדיווח על אירוע הגנת סייבר, הגדרת מתודולוגיה של תגובה לאירוע וחזרה לשגרה לאחר אירוע הגנת סייבר.
21. **תכנית הערכות לחירום** - מניעה או צמצום נזק הנובע מאירוע חריג בהיבט אבטחת מידע הכולל קריסת מערכות ו/או פגיעה במאגרי המידע של משרד האוצר והגדרת דרכי פעולה ובניית תכנית לניהול המשכיות תפקודית בעת קרות "אסון".
22. מצורפת רשימת מאגרי משרד האוצר כפי שרשומה כיום אצל רשם המאגרים. למען שלמות התמונה, יצוין כי בימים אלו, משרד האוצר עורך מיפוי של מאגרי המידע במשרד האוצר והסדרת רישומם, ובכלל זה מאגרי מידע שטרם נרשמו, אך פרויקט זה טרם הגיע לסיומו.

בכבוד רב ,

P:\Tmtalyal.jpg

אנט קליימן

ממונה על פניות הציבור וחוק חופש המידע