

פרק	נושא	ממצאים	המלצה	תגובת המבוקר
5	אסטרטגיה ומדיניות IT	<ul style="list-style-type: none"> <li>- מסמך האסטרטגיה שהועבר לביקורת הינו טיוטה ולא מסמך סופי. מסמך אסטרטגיה יש להביא לאישור הנהלת ההסתדרות.</li> <li>- לא קיים מסמך מדיניות IT</li> <li>- מסמך מדיניות אבטחת המידע לא אושר ע"י הנהלת ההסתדרות</li> </ul>	<ul style="list-style-type: none"> <li>- יש להכין מסמך מדיניות IT כנגזרת של אסטרטגיית המחשוב של הארגון.</li> <li>- יש לאשר את מסמך המדיניות בנושא אבטחת המידע ע"י הנהלת ההסתדרות.</li> </ul>	<p>סמנכ"ל טכנולוגיות מידע ודיגיטל מסר, כי מסמכי המדיניות והאסטרטגיה, שנכתבו במנהל טכנולוגיות מידע, נכתבו/אושרו על-ידו, כחבר בהנהלת ההסתדרות. בשנת 2022 יאוגדו הנהלים הקיימים למסמך מדיניות IT.</p>
6.2	מערך SIEM /SOC	<ul style="list-style-type: none"> <li>- הביקורת מצאה כי לא הוטמעה טכנולוגיית SIEM ממוכנת המקבלת נתונים ממערכות ארגוניות שונות, מנתחת אותם ומאפשרת בקרה על תהליכים ואירועים.</li> <li>- לא קיים בהסתדרות מערך SOC .</li> </ul>	<p>יש לפעול להקמת מערך SIEM/SOC, ובכלל זה למפות את המערכות שישולבו במערך בהתאם לרמת הסיכון.</p>	<p>סמנכ"ל טכנולוגיות מידע ודיגיטל מסר, כי בהסתדרות קיימת מערכת - ADAUDITPLUS המנטרת את מערכת ה- Directory Active מערכת לניהול משתמשים ושיתופי רשת. המערכת בניהול צוות ה- SYSTEM, עוברת בקרה ברמה שבועית ע"י יועצי אבטחת המידע וקיימות בה התראות המוגדרות במערכת. עם זאת, בתוכנית העבודה לשנת 2022, מתוכנן לרכוש שרותי SOC ולעבות את ה-SIEM .</p>
6.3	סקר הערכת סיכוני אבטחת מידע	<ul style="list-style-type: none"> <li>- לא בוצע סקר הערכת סיכוני אבטחת מידע לרבות מיפוי לכלל סיכוני אבטחת המידע</li> <li>- לא הוכנה תוכנית סקרים תקופתית בהתאם למיפוי האיומים</li> <li>- קיימות בקרות אבטחת מידע תקופתיות מתמשכות אשר מבוצעות על ידי יועצי אבטחת המידע, אולם אלה אינן מבוססות על סקר הערכת סיכונים מקדים ואינן מקיפות בהכרח את כלל הסיכונים</li> </ul>	<p>יש לבצע סקר הערכת סיכוני אבטחת מידע הכולל מיפוי סיכוני ואיומי אבטחת המידע ובהתאם להגדיר תוכנית סקרים ובקרות.</p>	<p>סמנכ"ל טכנולוגיות מידע ודיגיטל מסר, כי יפעל לבצע סקר הערכת סיכונים הממפה את סיכוני ואיומי אבטחת מידע בהסתדרות ובהתאם תוכן תוכנית סקרים רב שנתית.</p>

פרק	נושא	ממצאים	המלצה	תגובת המבוקר
6.4	גישה מרחוק	<ul style="list-style-type: none"> <li>בעמדות הקצה (המחשבים האישיים של העובדים או במחשבים הנישאים) לא הותקן רכיב HOST CHECKER אשר אמור לוודא כי העמדה עומדת בדרישות בסיס.</li> <li>ההסתדרות אינה מפעילה כלים לשם קבלת דיווח מעמדות הקצה בגין פעילות חריגה (כגון EDR- Endpoint Detection &amp; Response). כתוצאה מכך לא מתקיימת בקרה על פעילות חריגה.</li> </ul>	<ul style="list-style-type: none"> <li>הומלץ להתקין רכיב HOST CHECKER המודא כי עמדות הקצה עומדות בדרישות אבטחת מידע</li> <li>הומלץ לבחון התקנה בעמדות הקצה, המשמשות לגישה מרחוק, כלים לשם קבלת דיווח מעמדות הקצה בגין פעילות חריגה (כגון EDR- Endpoint Detection &amp; Response)</li> </ul>	<ul style="list-style-type: none"> <li>סמנכ"ל טכנולוגיות מידע ודיגיטל מסר כי, העבודה בחיבור מרחוק מבוצעת ע"י חיבור פורטלי של ה-FW-פורטי (לא משתמשים בחיבור RDP רגיל).</li> <li>אין חיבור בין המחשב המרוחק לרשת ההסתדרות, ולא ניתן להעביר קבצים בתקשורת.</li> <li>קיים זיהוי דו שלבי עבור כל משתמש בחיבור מרחוק מה שמפחית את הסיכון. יחד עם זאת, אנו נבחן שילוב כלים להגברת האבטחה לרבות HOST CHECKER ו-EDR.</li> </ul>
6.6	הצפנת מחשבים ניידים ורמת הרשאת העובדים	<ul style="list-style-type: none"> <li>ישנם כ-300 מחשבים ניידים בידי העובדים ואלה אינם מוצפנים - במצב של אובדן או גניבת מחשב נייד, כל המידע השמור בו עלול להיחשף</li> <li>משתמשי הקצה מוגדרים כמנהלי המחשב ובהתאם יכולים לבצע כל פעולה שהיא, כולל פעולות העלולות לסכן את הארגון</li> </ul>	<ul style="list-style-type: none"> <li>הומלץ להצפין את המחשבים הניידים</li> <li>הומלץ כי משתמשי הקצה לא יוגדרו כמנהלי המחשב על מחשביהם</li> </ul>	<ul style="list-style-type: none"> <li>סמנכ"ל טכנולוגיות מידע ודיגיטל מסר, כי לא ניתן להעתיק חומרים מתוך רשת ההסתדרות במחשב הנייד. לא קיימת אפשרות לבצע העתק/הדבק. העובדים עוברים הדרכות בנושא אבטחת מידע ובמיוחד בנושא שמירת מידע במחשבים הניידים.</li> <li>לתקציב 2022 הוכנס תקציב להטמעת מערכת MDM ונבחן נושא הצפנת המחשבים והסרת הגדרת משתמשי הקצה כמשתמשי ADMIN.</li> </ul>
6.7	מערכת דלף מידע	<ul style="list-style-type: none"> <li>לא קיימת בהסתדרות מדיניות דלף מידע. באופן זה לא הגדירה ההסתדרות מהם מסלולי דלף המידע האפשריים ומהם המענים ההולמים, שיש להעמיד מול כל איום.</li> </ul>	<ul style="list-style-type: none"> <li>יש להגדיר מדינות דלף מידע בארגון לרבות התייחסות לנושא גישה לרשת עם התקן USB</li> <li>יש לבחון מימוש מערכת תומכת, היכולה לאתר ולמנוע</li> </ul>	<ul style="list-style-type: none"> <li>סמנכ"ל טכנולוגיות מידע ודיגיטל מסר, כי בשנת 2015 בוצע מיפוי לכלל ערוצי התקשורת אשר מתעדכן ברמה שנתית. על בסיסו נקבעות הרשאות לגישה למידע.</li> </ul>

פרק	נושא	ממצאים	המלצה	תגובת המבוקר
		<ul style="list-style-type: none"> <li>- לא מומשה מערכת תומכת, היכולה לאתר ולמנוע דלף מידע בזמן אמת בערוץ שונים לרבות הדוא"ל</li> <li>- לא קיים נוהל סדור המגדיר מיהם הגורמים /תפקידים אותם יש לחסום ואילו לא אמורים להיחסם (בשימוש בהתקן USB)</li> </ul>	<p>דלף מידע בזמן אמת, לכל הפחות בערוץ הדוא"ל - המשמעותי ביותר</p>	<ul style="list-style-type: none"> <li>- נכתב נוהל לעובדים לגבי המותר והאסור והעובד חותם עליו.</li> <li>- קיימת מדיניות שימוש במדיה נתיקה ברשת ההסתדרות וכן קיימת מדיניות לחסימת CONTROL DEVICE בתחנות העבודה במערכת ההגנה TRENDMICRO בניהול משתמשים דרך מערכת ה-AD.</li> <li>- בשנתיים הקרובות, נתחיל במימוש מנגנוני DLP גם באופיס 365 בשנת 2022 תכתב מדיניות דלף מידע אשר בין השאר תתייחס לנושא חסימת התקני USB.</li> </ul>
7.1	מדיניות שימוש במוצרים - EOL	<ul style="list-style-type: none"> <li>- לא קיימת בהסתדרות מדיניות סדורה בנושא EOL לרבות הגדרות התנאים לשימוש במוצרים הנמצאים בשלב של EOL.</li> <li>- בארגון מותקנת מערכת הפעלה WIN 7 על כ-450 מחשבים מתוך 1290 - מערכת הפעלה זו נמצאת ב-EOL החל משנת 2020 ובהתאם אינה נתמכת במהלך הביקורת, מערכת ה-FORTINATE (ה-FW הארגוני) אינה נתמכת - ועדת הרכש שדנה בעלויות חידוש הרישיון נערכה בחודש מאי 2021 מועד בו הגרסה הקיימת בהסתדרות כבר לא נתמכה מספר חודשים. הביקורת לא זיהתה פעולה לשדרוג המערכת, טרם כינוס ועדת הרכש</li> </ul>	<p>יש להגדיר מדיניות שימוש במוצרי EOL המוודאת שדרוג מוצרים בטרם יגיעו למועד ה-EOL, וליישמה. במסגרת זו יש לפעול לעדכון ושדרוג מערכת ההפעלה WIN7 במחשבי ההסתדרות.</p>	<p>סמנכ"ל טכנולוגיות מידע ודיגיטל מסר כדלקמן:</p> <p>נושא WIN7 נמצא בטיפול. למועד מתן התגובה לביקורת קיימות כ-220 תחנות עבודה בהן מערכת הפעלה WIN7. קיימת התקדמות ברמת שדרוגים/החלפה של תחנות עבודה בהובלת צוות ה-IT ובליווי יועצי אבטחת המידע.</p> <p>בעקבות הביקורת, נכתבה ומיושמת מדיניות EOL, אשר תוודא כי תשתיות ומערכות יטופלו בזמן.</p>

תגובת המבוקר	המלצה	ממצאים	נושא	פרק
		<p>נמצא כי לא קיים מיפוי מלא של מערכות המידע בהסתדרות וכי לא בוצע הליך למיפוי וזיהוי כלל המערכות הקיימות בשרתי ההסתדרות לרבות במרחבים.</p> <p>יש לציין כי בעקבות הביקורת בוצע מיפוי, כאמור לעיל.</p>	מיפוי רכיבי חומרה ותוכנה	7.2
<ul style="list-style-type: none"> <li>- סמנכ"ל טכנולוגיות מידע ודיגיטל מסר כי המחלקה פעלה תקופה ארוכה באילוצים קשים של כ"א וניהול.</li> <li>- לאחר ניסיונות רבים לשיפור החלק הניהולי המחלקה פוצלה וניהול התמיכה הועבר למנהל אחר.</li> <li>- הוקמה מחלקה חדשה הנמצאת בתהליכי בנייה. בוצעה סדנת שירות מיוחדת כולל סיוע וחונכות למנהל החדש, כדי לבנות ולעמוד באמנת שירות, SLA, כנדרש.</li> </ul>	<ul style="list-style-type: none"> <li>- יש להגדיר בקרה למדידת עמידה ב-SLA כפי שמוגדר בנהלי מוקד ה-HELP DESK</li> <li>- יש לבצע בקרות לבחינת יעילות העובדים ב-HELP DESK</li> <li>- יש לעדכן ולתקן את דוחות המערכת</li> </ul>	<ul style="list-style-type: none"> <li>- לא התבצעה מדידה לעמידה ב-SLA שהוגדר לצורך בדיקת עמידה ביעדים, הפקת לקחים ושיפור תהליכים</li> <li>- לא התבצעה מדידה של יעילות הטיפול ברמת עובדי מערך ה-HELP DESK.</li> <li>- למשרד המבקר נמסר כי דוחות המערכת אינן תקינים ועל כן לא מתאפשר לבצע תהליכים אלו.</li> </ul>	מדידת עמידה ב-SLA	8.1
<ul style="list-style-type: none"> <li>- סמנכ"ל טכנולוגיות מידע ודיגיטל מסר כי המחלקה פעלה תקופה ארוכה באילוצים קשים של כ"א וניהול.</li> <li>- לאחר ניסיונות רבים לשיפור החלק הניהולי המחלקה פוצלה וניהול התמיכה הועבר למנהל אחר.</li> <li>- הוקמה מחלקה חדשה הנמצאת בתהליכי בנייה. בוצעה סדנת שירות מיוחדת כולל סיוע וחונכות למנהל החדש, כדי לבנות ולעמוד באמנת שירות, SLA, כנדרש.</li> </ul>	<ul style="list-style-type: none"> <li>- יש לבצע מעקב אחר שיחות ננטשות, כולל הגדרת מדיניות בנושא חזרה לשיחות אלו.</li> </ul>	<p>במוקד ה-HELP DESK מתקבלות בין 5,000 ל-8,000 פניות בממוצע, בשנה. שיחות ננטשות הינן שיחות שנותקו לפני שהגיעו למענה אנושי.</p> <p>מעקב אחר השיחות הננטשות מאפשר לארגון לשפר ולפתח את אופן חיזוי עתות העומס במוקד, הצבת כמות נציגים רבה יותר בזמני עומס ובחינת נתב השיחות.</p>	בקרת שיחות ננטשות במוקד ה-HELP DESK	8.2

פרק	נושא	ממצאים	המלצה	תגובת המבוקר
9.1	בקשות לפיתוח ושינויים במערכות המידע	<ul style="list-style-type: none"> <li>- ניהול הפיתוחים בהסתדרות נעשה באמצעות קובץ אקסל ולא באמצעות מערכת ניהול שינויים כמקובל ביחידות פיתוח. הקובץ בעל תיעוד חסר.</li> <li>- לא מתקיימים תהליכים למדידת התשומות שהשקיעו עובדי מערך הפיתוח במשימות שבוצעו ובהתאם לא מתבצעת בקרת תקציב מול ביצוע</li> <li>- משרד המבקר התרשם כי כמות המשימות העומדות בפני מנהל מערכות מידע ודיגיטל הולכת ומתרבה במהלך השנים - המשימות דורשות היקפי עבודה רחבים ממצבת העובדים במחלקה.</li> </ul>	<ul style="list-style-type: none"> <li>- יש לבחון יישום והפעלת מערכת ניהול שינויים.</li> <li>- יש להקפיד על מילוי נתונים עדכני ברישומי המחלקה.</li> <li>- יש לבחון את הדרכים למדידת התשומות אל מול תקציבי המשימות.</li> <li>- מומלץ לבצע תהליכי תקנון, הבחנים לעומק את כמות המשימות הנדרשת למול כוח האדם הקיים.</li> </ul>	<ul style="list-style-type: none"> <li>- סמנכ"ל טכנולוגיות מידע ודיגיטל מסר כי מערכת ה-MONDAY לניהול פיתוחים, כבר הותקנה במנהל מחשוב ומתחילים לעבוד איתה. המערכת תשדרג את יכולות הניהול שיבוצעו באופן אוטומטי ולא ידני.</li> <li>- מדידת התשומות ברמת משימה - אינו ישים, לאור כמות המשימות והמשאבים שעומדים לרשותנו. הדבר יישקל שוב בעתיד</li> </ul>
9.2	בקרת גישה לייצור	<ul style="list-style-type: none"> <li>- נמצאו 10 אנשי IT בעלי הרשאות עדכון במערכת הייצור של מערכת תפנית. לעיתים מבוצעים עדכונים ישירים על בסיס הנתונים.</li> <li>- לא קיימים תהליכים לאישור ובקרת פעולות בסביבת הייצור על מנת לוודא שהללו בוצעו בכפוף לאישור.</li> <li>- נמצא כי מפתחי חברת "מטריקס" (היושבים בהרצליה) הם בעלי גישה קבועה לסביבת הייצור - ברמה הנוהלית עליהם לפתוח קריאת שירות טרם כניסתם למערכת - בפועל לא קיימת מגבלה על גישתם.</li> <li>- גישת משתמשי חברת "מטריקס" מרחוק אינה כוללת FA2. הללו התחברים מרחוק באמצעות קו VPN באמצעות שם משתמש וסיסמה בלבד.</li> </ul>	<ul style="list-style-type: none"> <li>- יש להסיר הרשאות של אנשי IT לסביבת הייצור - במידה וקיים צורך תפעולי יש לתת הרשאות אלו באופן נקודתי.</li> <li>- יש להגדיר בקרה המוודאת, כי גישת המפתחים לסביבת הייצור, בוצעה רק לאחר אישור של גורם רלוונטי, לרבות מפתחים היושבים בהסתדרות או אלו הניגשים מרחוק.</li> <li>- יש להגדיר בקרת FA2 בגישת משתמשי "מטריקס" לרשת ההסתדרות.</li> </ul>	<ul style="list-style-type: none"> <li>- סמנכ"ל טכנולוגיות מידע ודיגיטל מסר, כי מערכת התפנית בנויה ממודולים שונים כגון. לכל תחום במערכת יש מומחים ייעודיים, שמטפלים בנושא ולכן יש ריבוי משתמשים.</li> <li>- במקרים חריגים ביותר, יש צורך לעדכן נתון זה או אחר בבסיס הנתונים - הדבר מתבצע תחת פיקוח קפדני ולאחר אישורים מתאימים.</li> <li>- האגף נמצא בתהליך בנייה של בקרות מתאימות ביחד עם חברת "מטריקס" ויועץ אבטחת המידע, כולל יישום FA2, לכל הארגון.</li> </ul>

פרק	נושא	ממצאים	המלצה	תגובת המבוקר
		-		
10.2	הערכות לחירום (DRP)	בהסתדרות לא קיים מערך DRP להעלאת המערכות ונתוני הארגון בשעת חירום. נציין כי ממצא זה עלה גם בסקר סיכונים שבוצע בשנת 2020.	יש לוודא כי מוקם בהסתדרות מערך DRP, בהקדם.	סמנכ"ל טכנולוגיות מידע ודיגיטל מסר, כי החלה פעילות בנושא DRP בענן ציבורי. הנושא הוכנס לתקציב לשנת 2022.
10.3	שחזור קבצים	לא מבוצעים תהליכי שחזור סדורים ויזומים של מידע הקיים בקלטות הגיבוי, על מנת לוודא כי בשעת הצורך נתונים אלו יהיו זמינים ותקינים, בניגוד למפורט בנוהל הגיבויים.		במהלך הביקורת הנוכחית ובעקבותיה, החל מערך ה-IT לבצע שחזורים יזומים, כחלק מבקורות אבטחת המידע.
11	רכש טכנולוגי	<ul style="list-style-type: none"> <li>- ההסתדרות לא הגדירה את מטרות השימוש במחשבים הניידים עליהם מתקבלות הצעות מחיר מספקים. עלה כי נרכשו מחשבים נישאים בעלי מפרט גבוה יחסית עבור עבודה משרדית.</li> <li>- נמצא כי מאז 2016 לא נבחנו עלויות ההדפסה וחלופות להוזלת העלויות.</li> <li>- לא נמצא תיעוד לבקרה המתבצעת לנכונות החיובים, שהעבירה חברת מ. בגין עובדיה.</li> </ul>	<ul style="list-style-type: none"> <li>- יש לוודא כי הצעות המחיר לרכש מחשובי, המועבר לוועדת הרכש, יבוצעו על סמך מטרות שימוש, שיוגדרו לטובין הנרכש ואל מול benchmark נהוג בשוק.</li> <li>- מומלץ לבצע תהליכים תקופתיים לבחינת יעילות ההתקשרות עם ספק המדפסות, לאור העלויות הגבוהות והדינמיות הקיימת בשוק זה.</li> <li>- יש לתעד את הבקרה, לבדיקת נאותות דיווח שעות הנוכחות של עובדי חברת מ. בחשבוניות המוגשות לתשלום.</li> </ul>	<ul style="list-style-type: none"> <li>- סמנכ"ל טכנולוגיות מידע ודיגיטל מסר כי המחשבים בהסתדרות מיועדים לעובדים שמצויים רוב הזמן מחוץ למשרד - בביקורים במקומות העבודה (סביבות אגרסיביות), כמו כן, המחיר כולל תמיכה ושירות של 5 שנים בבית הלקוח.</li> <li>- בהסתדרות קיימת תוכנית PapelessOffice (ארגון ללא נייר) שהוצגה להנהלת ההסתדרות בשנת 2019. מסיבות שונות, הוחלט לא ליישמה.</li> <li>- בתחילת שנת 2022 נצא למכרז חדש למדפסות - שיכלול שינוי המודל העסקי מרכש, לשכירות תפעולית. במקביל תבחן גם הקטנת עלויות ההדפסה.</li> <li>- במהלך הביקורת ובעקבותיה, יושמה בקרה, לתיעוד נאותות דיווח השעות, בחשבוניות המועברות מחברת מ.</li> </ul>

תגובת המבוקר	המלצה	ממצאים	נושא	פרק
למועד תום הביקורת נמסר מהמנהל למערכות מידע ודיגיטל, כי בעקבות הביקורת הוכנה תוכנית הדרכות לשנת 2022.		<ul style="list-style-type: none"> <li>- בשנים המבוקרות לא התקיימו הדרכות והכשרות לצוות ה-HELP DESK.</li> <li>- לא קיימת תוכנית הדרכות סדורה לעובדי מחלקת מערכות מידע ודיגיטל.</li> </ul>	מקצועיות והכשרות	12
סמנכ"ל טכנולוגיות מידע ודיגיטל מסר, כי האגף פנה לקבלת חוות דעת של יועץ ביטוחי, אשר <b>אכן</b> המליץ לבחון רכישת כיסוי ביטוחי לנזקי סייבר. הנושא ייבחן במהלך שנת 2022.	לאור שכיחות נזקי אירועי סייבר בשנים האחרונות, הומלץ לבחון רכישת כיסוי ביטוחי לנזקי סייבר.	למועד הביקורת לא קיים להסתדרות כיסוי ביטוחי לנזקי סייבר - נזקים העלולים להגרם בעקבות אירועי דלף מידע, פגיעת וירוסים וכדי אינם מכוסים בפוליסת הביטוח הקיימת ("ביטוח ציוד אלקטרוני") של ההסתדרות.	ביטוח	13