# תוכן עניינים

## 1. כללי

1.1 תרחיש הייחוס למתקפת סייבר על מערכות רכבת ישראל כתוצאה מתקיפת שרשרת האספקה, יכול להתממש באמצעות ערוצי תקיפה מגוונים ביותר, כגון חדירה למערכות של ספק בעל רמת הגנה נמוכה יחסית ודרכו חדירה למערכות החברה; שימוש בעדכוני תוכנה לגיטימיים להפצת נוזקה וכו'.

1.2 תרחיש הייחוס אינו מפרט איומים תיאורטיים, אלא מבוסס ניתוח המסתמך על מספר רב של אירועים שהתרחשו בארץ ובעולם, שמהותם היא פגיעה בארגונים, תוך ניצול שרשרת האספקה שלהם.

1.3 פעילותה השוטפת של חברת רכבת ישראל מערבת ספקים חיצוניים רבים, המספקים לה שירותים שונים. במסגרת השירותים ספקים אלה עשויים ליצור ולקבל מידע מ/עבור רכבת ישראל, לספק תשתיות לאחסון ועיבוד המידע, או לקבל גישה לרשת רכבת ישראל ולמידע שלה.

1.4 נכסי המידע של רכבת ישראל מסווגים כמידע פומבי/ פנימי/ רגיש עסקי/ רגיש אישי, ודליפתם לגורמים בלתי מורשים עלולה לגרום לסיכון ביטחוני או לנזק עסקי, תדמיתי או משפטי משמעותי לרכבת ישראל.

1.5 על-מנת למזער את הסיכונים לפגיעה בסודיות, באמינות ובזמינות המידע, נדרש להגן על נכסי המידע, הן כאשר הם מצויים על גבי ברשת רכבת ישראל והן כאשר הם מצויים אצל הספקים או באחריותם.

1.6 מסמך זה יפרט הנחיות ודרישות אבטחת מידע לספקים שיוצרים, מעבדים ו/או מחזיקים מידע של רכבת ישראל בתשתיות המחשוב שלהם.

1.7 נספח זה אינו עוסק בנושא חיבור מרחוק לתשתית המערכות החיוניות ולמערכות הבקרה ברכבת ישראל.

1.8 פירוט הדרישות ותיאור תהליך אישור חיבור ספקים חיצוניים למערכות פנימיות של רכבת ישראל, מפורט בנוהל "חיבור מרחוק של קבלנים חיצוניים למערכות של רכבת ישראל לצרכי תמיכה".

1.9 מסמך זה מהווה נספח סייבר בהתקשרויות הרכבת עם ספקיה.

## 2. הגדרות

2.1 "**ספק**": גוף חיצוני- על כל עובדיו וספקי המשנה שלו, המספק לרכבת ישראל שירותים (לרבות שירותי מיקור חוץ-Outsourcing), או טובין, באשר הם.

2.2 "**סייבר**" ("**המרחב הקיברנטי**"): המתחם הפיזי והלא פיזי שנוצר, או מורכב, מחלק, או מכל הגורמים הבאים: מערכות ממוחשבות, רשתות מחשבים ותקשורת, טכנולוגיה תפעולית (OT), תוכנות, מידע ממוחשב, תוכן שמועבר באופן ממוחשב, נתוני תעבורה ובקרה, לרבות הרובד האנושי. (האנשים המשתמשים בכל אלה).

2.3 "**הגנת סייבר**": כל הפעולות שתכליתן להגן על נכסי המידע של רכבת ישראל במרחב הסייבר.

2.4 "**מתקפת סייבר**": תקיפה במרחב הסייבר המסכנת נכסי סייבר, מערכות ותשתיות הנתמכות על ידם.

2.5 "**אירוע סייבר**": התרחשות אשר מעידה על פגיעה אפשרית בפעילותו התקינה של נכס סייבר, שקיים יסוד להניח, כי היא נובעת מפעילות מכוונת במרחב הסייבר.

2.6 "**נכנס מידע**": קובץ, רשומה, מאגר נתונים או עותק פיזי, המכיל מידע שנוצר או התקבל במסגרת הפעילות השוטפת של החברה, ובעל ערך לתפקודה התקין של רכבת ישראל.

2.7 "**מידע מוגן**[1]":
כל אחד מאלה:

2.7.1 מידע שחוק הגנת הפרטיות, תשמ"א 1981, חל עליו.

2.7.2 מידע אודות ארגון שאינו נחלת הכלל.

2.7.3 סודות מסחריים לפי חוק עוולות מסחריות, תשנ"ט- 1999.

2.8 "**נכס סייבר חיוני**"נכס סייבר אשר תפקודו התקין נדרש לשם הבטחת רציפות תפקודה של רכבת ישראל כנכס סייבר לאומי- חיוני במדינת ישראל. בהגדרה זו נכללים: מערכות התפעול, מערכות בקרה תעשייתיות (ICS[2]), רשתות מחשבים חיונית לתפעולה השוטף של רכבת ישראל בשגרה ובחירום. בנוסף, בהגדרה זו נכללים כל נתון ו/או מידע (לרבות תכתובת), הקשורים למערכות אלו.

2.9 "**סביבת המידע של רכבת ישראל" (אצל הספק)**: נכסי המידע של רכבת ישראל וכל התשתיות, תחנות הקצה והרכיבים המאפשרים גישה אליהם, או שבהם הם נוצרים, נשמרים, מעובדים או מועברים.

2.10 "**צורך עסקי**": הצורך הנובע מתפקיד העובד ו/או מהמשימות המוטלות עליו לצורך ביצוע השירותים עבור רכבת ישראל.

2.11 "**סודיות" (Confidentiality)**: דרישה שהגישה למידע תוגבל אך ורק לגורמים שהוגדר שתפקידים מחייב גישה זו, וניתנו להם הרשאות בהתאם.

2.12 "**שלמות ואמינות" (Integrity)**: דרישה שהמידע יהיה שלם, אמין ומדויק לכל אורך מחזור חייו.

2.13 "**זמינות" (Availability)**: דרישה שהמידע יהיה זמין למשתמשים המורשים כאשר הם זקוקים לו.

2.14 "**תווך מאובטח" (Secure Channel)**: יצירת תוואי תקשורת מאובטחת למניעת התערבות, צפיה בלתי מורשית ואו שיבוש נתונים.

2.15 "**הצפנה**": יישום של קריפטוגרפיה הממירה מידע גלוי (Clear Text) למידע מקודד (Cipher Text), באופן שיוכל להיות מפוענח ומובן אך ורק לגורמים מורשים.

2.16 "**HLD**": תכנון פתרון מותאם לאתרי/מערכות הלקוח ובחינת היתכנות של הפתרון ברמת ארכיטקטורה, היבטי סייבר, תשתיות תקשורת, רכיבי חומרה, ציוד, אביזרים, ממשקים, תוכנה ותצורת מערכת.

2.17 "**LLD**": תכנון ארכיטקטורה מעמיק, רשימות ציוד ויצרנים, אפיון מפורט של הממשקים ותוכנית המימוש.

---

[1] הגדרת מערך הסייבר הלאומי

[2] "**מערכת בקרה תעשייתית**": (ICS-Industrial Control System) מערכת מבוססת מחשוב, המנטרת ומבקרת תהליכים המתחוללים בתוך מערכת יצור תעשייתית.

2.18 "**אמצעי זיהוי**": אמצעי המספק פרטים לגבי זהותו של אדם, או מערכת, בעת ניסיון כניסה ואישור ביצוע פעולות מטעמם למערכת מידע.

2.19 "**גישה מרחוק**": התחברות משתמשים וספקים מחוץ לתשתית הארגון לטובת קבלת גישה למערכות/שרתי /תחנות קצה וכו' והקבצים שבהם השייכים לרכבת ישראל, לצורכי עבודה של משתמשי הארגון ותחזוקה המבוצעת ע"י ממשקים עסקיים (ספקים/קבלנים).

## 3. אבטחת מידע

### 3.1 **סודיות והגנה על פרטיות**

3.1.1 הספק מצהיר שידוע לו כי מידע ומסמכים שימסרו לו ו/או למי מטעמו, על ידי רכבת ישראל במהלך מתן השירות לפי הסכם זה, מוגדרים כ"רגישים" ואין לפרסמם, או לעשות בהם שימוש, אלא לצורך מתן השירות עפ"י ההסכם.

3.1.2 הספק מתחייב לשמור בסוד ולא להעתיק, להודיע, למסור, או להביא לידיעת כל אדם כל ידיעה שתגיע, או שהגיעה אליו ו/או למי מטעמו, תוך כדי, או עקב ביצוע השירותים.

3.1.3 הספק מתחייב לשמור על סודיות המידע והמסמכים המפורטים לעיל, גם לאחר תום תקופת ההתקשרות, בהתאם להסכם זה.

3.1.4 הספק מתחייב להחתים את עובדיו ונותני השירותים מטעמו לרבות קבלני המשנה על הצהרת התחייבות לשמירת סודיות מתאימה וטופס העדר ניגוד עניינים, בהתאם לדרישות רכבת ישראל.

3.1.5 אין להעתיק, לפרסם, להעביר, להודיע, למסור, או להביא לידיעת כל אדם אחר, בין אם במישרין ובין אם בעקיפין, בין אם במעשה ובין אם במחדל, כל פריט מהמידע ו/או הסודות המקצועיים של רכבת ישראל אשר יגיע לידיו, לרשותו, או לידיעתו, באופן ישיר או עקיף, בקשר למתן השירות.

3.1.6 הספק מתחייב לשמירת סודיות באשר לכל הידע, שיטות העבודה, הציוד, המכשור, תצורת (קונפיגורציית) הרשת ומערך הגנת הסייבר, פרטי ומבנה הציוד המחשובי לרבות היצרנים והדגמים, הרכיבים וההתקנים, לרבות היצרנים והדגמים המצויים ברכבת ישראל, או שרכבת ישראל שוקלת את השימוש בהם בעתיד.

3.1.7 הספק מתחייב להביא את הוראות החוק והוראות סעיף זה לידיעת כל האנשים המועסקים על ידו, לשם ביצוע הסכם זה ו/או בקשר עמו.

3.1.8 הספק מתחייב לנקוט את האמצעים הדרושים על מנת לשמור על פרטיות הפונים, על פרטיהם ופרטי פנייתם, כנדרש על פי כל חוק, כן מתחייב הספק להדריך את עובדיו ביחס להגנה על פרטיות המידע והפונים ולהחתימם על התחייבות מתאימה.

3.1.9 הספק מתחייב למלא אחר כל הנחיות אגף הסייבר, הנחיות האבטחה והביטחון שיינתנו על ידי אגף ביטחון וחירום ברכבת ישראל וכן בהתאם לצורך, הנחיותיו של כל גורם מוסמך אחר ברכבת ישראל. (למען הסר ספק - רכבת ישראל לא תישא בעלויות יישום הנחיות אלו). האמור בסעיף זה הינו בכפוף לחובותיו הרגולטוריות של הספק.

3.1.10 הספק, עובדיו ונותני השירותים מטעמו מתחייבים להשתתף (במידת הצורך) בהדרכת/תדריך הגנת סייבר, שתוכנה יקבע על ידי אגף הסייבר ברכבת ישראל.

## 3.2 **דרישות כלליות**

3.2.1 הספק יתחייב לממש במלואם את התנאים העיקריים להלן:

3.2.2 הספק מתחייב לעמוד ולציית בכל הוראות חוק המחשבים, תשנ"ה-1995 וחוק הגנת הפרטיות, תשמ"א-1981 והתקנות שתוקנו מכוחו; וכן לציית לתנאים ותקנות עתידיים בנושא טיפול במערכות מידע ממוחשבות.

3.2.3 הספק מתחייב במסמך זה להיערך לפני תחילת מתן השירותים, למלא אחר כל דרישות והנחיות אגף הסייבר המפורטות בנספח זה, לרבות הנדרש בחוק הגנת הפרטיות, ובתקנות שהותקנו מכוחו מנותן שירותים חיצוני וממחזיק מאגרים מוגנים וממחויבויות רכבת ישראל, מכוח חוקי המדינה והוראות גורמי ההנחיה.

3.2.4 הספק יתחייב לניהול שוטף ומבוקר של השירותים הנדרשים, באופן מאובטח וממודר ולמניעת הגישה הפיזית לתחנות העבודה, לחדרי השרתים ולתשתית התקשורת המשמשת לעבודה מול רכבת ישראל-לגורמים שאינם מורשים.

3.2.5 ימונה נאמן הגנת סייבר מטעם הספק, אשר יונחה ע"י אגף הסייבר ברכבת ישראל ויהווה איש קשר(POC) לנושא ההגנה במרחב הסייבר.

3.2.6 הספק יעניק לנאמן הגנת הסייבר את כל הסמכויות, הכלים והאמצעים הנדרשים לביצוע תפקידו, לרבות סמכויות אכיפה על עובדי הספק בתחום הגנת הסייבר, והכל בכפוף להוראות והנחיות רגולטוריות החלות על הספק.

3.2.7 הרכבת תהיה רשאית להגדיר דרישות נוספות ו/או חלופות נוספות אל מול הספק.

3.2.8 בהתאם ללוח הזמנים והנחיות נוספות שיקבל הספק מנציגי הרכבת:

3.2.8.1. על הספק לספק תיאור מפורט, לרבות מסמך טופולוגיה, של כלל מערכות הIT והIOT/IIOT, הקיימות במערכת, תיאור זרימת הנתונים ואמצעי אבטחת המידע הקיימים.

3.2.8.2. הספק יציג פתרון מימוש למניעת גישה לוגית למערכת ולמרכיביה, לתשתיות ולמערכות המקושרות אליה.

3.2.8.3. הספק יציג את תפיסתו למימוש שכבות ההגנה הפיסית על ציוד המערכת בתוך מתקני רכבת ישראל, לרבות מידור פיזי לגישת טכנאים לציוד, גישה לחדרי הבקרה ואמצעי אבטחה והקשחה של מתקניו מחוץ לחצרי רכבת ישראל וכן את אמצעי האבטחה הפיזית והמידור שהוא נוהג לממש בפרויקטים דומים.

## 3.3 **הגנה על נכסי סייבר חיוניים ותשתית IT וOT**

3.3.1 לא תותר התחברות ישירה, או ניסיון להתחברות ישירה של טכנאים ונציגי ספקים אל מערכות חיוניות (נכסי סייבר חיוניים, כהגדרתם ע"י רכבת ישראל).

3.3.2 ככלל, לא יאושר חיבור מרחוק לתשתית המערכות החיוניות ולמערכות הבקרה ברכבת ישראל. מקרים חריגים ייבחנו בנפרד, על פי צורך ע"י יחידת הסייבר ברכבת ישראל.

3.3.3 בכל רכש המיועד לרשתות, אמצעי הגנה (מסוג חומרה ותכונה), תשתית מערכות חיוניות, ומערכות הבקרה התעשייתיות ברכבת ישראל, יהיו כפופים לאישור אגף הסייבר ברכבת ישראל.

3.3.4 רכיבי תוכנה- ייבדק הצורך בביצוע מבדקי חוסן/חדירות טרם התקנתם, בהתאם להנחיות מחייבות, אשר יועברו ע"י אגף הסייבר ברכבת ישראל.

3.3.5 על הספק להתחייב לדווח בכתב ובאופן מיידי, למרכז הניטור הקיברנטי ברכבת ישראל בטלפון: 08-6533065 אודות כל התרחשות חריגה במתחמי הספק ו/או פגיעה, או ניסיון לפגיעה, ברכיבי האבטחה, גניבה, או ניסיון לגניבה של רכיבים המתוכננים להתקנה במערכות הקריטיות (נכסי סייבר חיוניים).

3.3.6 לא יתאפשר חיבור מחשבים, טלפונים, מצלמות, רכיבי זיכרון נייד (Disk On Key), או כל אמצעי מחשוב, או אחסון אחר, אל מערכות חיוניות ומערכות בקרה תעשייתיות(ICS), לרבות לצורך טעינת מכשירים סלולאריים/אחרים. במקרה הצורך ולאחר קבלת אישור פרטני-מראש ע"י מנהל אגף הסייבר ברכבת ישראל, יותר שימוש חד-פעמי ברכיב זיכרון נייד ייעודי ו/או מחשב נייד ייעודי.

## 3.4 <u>ניהול אבטחת מידע, רגולציה ותקינה- דרישות חובה</u>

3.4.1 בהתאם ללוח הזמנים והנחיות נוספות שיקבל הספק מנציגי הרכבת הספק יגדיר מדיניות אבטחת מידע התואמת חוקים, רגולציות ותקנים רלוונטיים לגביו, ההולמת את הסטנדרטים המקובלים בתחום. המדיניות תאושר ע"י דרג ניהולי בכיר ותוטמע בקרב כל הגורמים בעלי גישה לסביבת המידע של רכבת ישראל.

3.4.2 לספק קיימים נהלי אבטחת מידע לכל הפחות בנושאים הבאים:

3.4.2.1. אירועי אבטחת מידע, ניהול תגובה, תחקור וכו';

3.4.2.2. אבטחה מידע במשאבי אנוש וניהול מחזור חיי עובדים (קבלה, עזיבה, הדרכות וכו');

3.4.2.3. אבטחת נכסי מידע של לקוחותיו;

3.4.2.4. אבטחת יישומים של הלקוח;

3.4.2.5. פיתוח מאובטח ותחזוקה של המערכות.

3.4.3 ככל ורלוונטי, הספק נדרש לעמידה מלאה בתקן PCI-DSS.

## 3.5 <u>אבטחת מידע במשאבי אנוש-דרישות חובה</u>

3.5.1 הספק אחראי לבצע בדיקות רקע לעובדיו המורשים לסביבת המידע של רכבת ישראל, בכפוף למגבלות החוקים הרלוונטיים (לדוגמא, הנחיות משטרת ישראל, תעודת יושר, בדיקות רקע פנימיות של רכבת ישראל או כל בדיקה אחרת המאושרת כל על ידי רשויות החוק).

3.5.2 הספק יבצע פעילויות להעלאת מודעות עובדיו לנושאי אבטחת מידע, הגנת הפרטיות ולסיכונים הרלוונטיים לביצוע תפקידם בפרט. על הספק לוודא את בקיאות עובדיו בנושאים אלו, בין היתר על ידי מבחני אפקטיביות שתוצאותיהם יועברו אל רכבת ישראל.

3.5.3 הספק יוודא ביטול הרשאות והחזרת ציוד ומצעי מידע שמכילים מידע של רכבת ישראל, בעת עזיבת עובד או שינוי תפקיד.

## 3.6 <u>העברת מידע רגיש/חסוי בין הספק ורכבת ישראל- דרישות חובה</u>

3.6.1 מידע דיגיטלי לא יועבר באמצעות רשת האינטרנט או במייל רגיל בין הספק ורכבת ישראל או בין הספק וספקי משנה, אלא בערוץ מאובטח, כפי שיימסר במועד ההעברה ע"י איש הקשר של הספק ברכבת ישראל.

3.6.2 מידע על-גבי אמצעים פיזיים (עותק קשיח, מדיה נתיקה) יימסר ישירות לידי עובד רכבת ישראל או בתהליך שיוגדר במועד העברה ע"י איש הקשר של הספק ברכבת ישראל.

3.6.3 יש להצפין מידע המועבר על-גבי מדיה נתיקה. מפתח הצפנה יימסר בנפרד לצד המקבל.

3.6.4 בעת העתקת מידע למדיה נתיקה ע"י ספק משנה, יש לוודא מחיקה אפקטיבית של כל העותקים מתשתיות המחשוב של ספק המשנה.

## 3.7 <u>אחסון מידע- דרישות חובה</u>

3.7.1 ככלל, המידע של רכבת ישראל יאוחסן בשרתים ברשת הפנימית של הספק, ולא בתחנות הקצה.

3.7.2 במקרים בהם החומרים הוגדרו רגישים ע"י רכבת ישראל כלל המידע יישמר באופן מוצפן וזאת ע"י אמצעי ותקני הצפנה מקובלים.

3.7.3 במקרים בהם יש צורך עסקי לשמור מידע רגיש של רכבת ישראל במחשב נייד, יש להצפין את הקבצים או את הכונן הקשיח של המחשב.

3.7.4 בסיום ההתקשרות עם רכבת ישראל, הספק יוודא העברת כל המידע לרכבת ישראל ומחיקה לצמיתות של כל ההעתקים שלו משרתי הספק. יש לשמור תיעוד (לוג) של מחיקת המידע. האמור בסעיף זה כפוף לחובותיו הרגולטריות של הספק.

## 3.8 <u>גיבוי והתאוששות- דרישות חובה</u>

3.8.1 המערכת תיבנה לרמת זמינות גבוהה (99.999%).

3.8.2 הספק ידאג לגיבוי המידע של רכבת ישראל. גיבויים המכילים מידע רגיש יישמרו באופן מאובטח, מוגן מפני שכתוב ומוצפן. הגישה לגיבויים תתאפשר רק לפי צורך עסקי.

3.8.3 יש לאחסן את מפתחות ההצפנה לגיבויים בנפרד מהמדיה.

3.8.4 הספק יתחזק תכניות המשכיות עסקית והתאוששת מאסון, אשר תתמוך בהמשך הפעילות העסקית עבור נכסי ומערכות רכבת ישראל.

## 3.9 **אבטחת רשת- דרישות חובה**

3.9.1 בהתאם ללוח הזמנים והנחיות נוספות שיקבל מנציגי הרכבת, הספק יעביר תכנון HLD הכולל את תצורת המערכת תיאור סביבות העבודה, זרימת המידע, פרוטוקולים בשימוש ואמצעי אבטחת המידע.

3.9.2 בהתאם ללוח הזמנים והנחיות נוספות שיקבל מנציגי הרכבת, הספק יעביר תוכנית LLD הכוללת תכנון ארכיטקטורה מעמיק, רשימות ציוד ויצרנים, אפיון מפורט של הממשקים ותוכנית המימוש.

3.9.3 לא תתאפשר גישה ישירה מרשת האינטרנט לסביבת המידע של רכבת ישראל אלא באמצעות קישור מאובטח ושימוש בהזדהות דו שלבית.

3.9.4 הספק יעביר לידי רכבת ישראל את רשימת הציודים בפרוייקט, הרשימה תכלול את שם היצרן, דגם הציוד, כמויות וגרסת תכנה.

3.9.5 הספק יפעל לעדכון והקשחות כלל הציודים בפרויקט ובדגש על שינוי הגדרות ברירת מחדל בכל הקשור לאבטחת מידע.

3.9.6 סביבת המידע של רכבת ישראל תהיה מוגנת באמצעות מנגנוני אבטחת המידע הבאים לפחות:

3.9.7 NAC-Network Access Control

3.9.8 Network Firewall- תתאפשר תעבורה לפי צורך עסקי בלבד.

3.9.9 Gateway Anti-Malware Engines.

3.9.10 Web/Category based filtering.

3.9.11 Intrusion Prevention/Detection System (IPS/IDS).

3.9.12 Web Proxy Servers.

3.9.13 DDOS Protection.

3.9.14 Application Firewall- (עבור אפליקציות החשופות לאינטרנט).

3.9.15 Data Base Firewall- להגנה על בסיסי הנתונים.

3.9.16 SIEM- שימוש במערכת מרכזית לאיסוף בעלת יכולת קורלציה

3.9.17 יישום מערכת הלבנה הכוללת סריקות קבצים באמצעות מספר מנועי אנטי וירוס ויכולות CDR, בעת קליטת קבצים למערכת.

3.9.18 Data Loss Prevention – DLP.

3.9.19 תחנות קצה ושרתים בעלי גישה למידע השייך לרכבת ישראל יהיו מוגנות באמצעות תוכנות Endpoint Protection ו- Endpoint detection & Response.

3.9.20 יישום מערכת לניהול משתמשים חזקים(Admin)- PSM-Privileged Session Manager, PIM-Privileged Identity Manager, וכן בקרה לניטור והקלטות מסך לניטור פעילות משתמשים אלו בכל סביבת המידע של רכבת ישראל. הקלטות המסך ישמרו באופן מוגן מפני שינוי

ומחיקה לפחות ל-6 חודשים ויהיו זמינים לבקשת רכבת ישראל בכל עת.

3.9.21 WIFI לצרכים תפעוליים

3.9.21.1. סביבת ה-WIFI תופרד באופן מוחלט מסביבות העבודה אשר אינן רלוונטיות ועל בסיס הצורך לדעת.

3.9.21.2. יש להחליף את סיסמאות ברירת המחדל של הנתבים האלחוטיים באופן שיתאמו את דרישות המינימום המפורטות בפרק מדיניות סיסמאות.

3.9.21.3. לא יתאפשר ניהול מרחוק של הנתבים האלחוטיים (מחוץ לרשת רכבת ישראל).

3.9.21.4. השירות יאופשר לאחר קבלת אישור מקדמי ממנהל אגף הסייבר ברכבת ישראל ויותנה בביצוע פעולות נוספות על המפורט להלן.

3.9.21.5. נדרש יישום הזדהות חזקה בין רכיבי הקצה ל-Access Point, נדרש לכלול הצפנה בצירוף סיסמא מורכבת.

3.9.21.6. נדרש לאשר מול אגף הסייבר ברכבת ישראל את הפרוטוקולים המיושמים בתקשורת ה-WIFI ואת אופן אבטחתם.

3.9.21.7. נדרש ליישם שמירת לוגים וניטור לרשת ה-WIFI.

## 3.10 <u>הפרדת סביבות- דרישות חובה</u>

3.10.1 עבור סביבת העבודה ונתוני רכבת ישראל, הספק יקים תשתית ייעודית ונפרדת מתשתית הייצור של הספק וכן מתשתיות שאר לקוחותיו, התשתית שתוקם תופרד פיזית או לוגית ע"פ ההנחיה של אגף הסייבר ברכבת ישראל, למען הסר ספק, תצורת ההתקנה תקבע לאחר אישור LLD שיועבר לאגף הסייבר ברכבת.

3.10.2 בסיסי הנתונים של הרכבת יופרדו באמצעות שרת ייעודי ולא כהפרדה לוגית ברמת בסיסי הנתונים.

3.10.3 יבוצע מידור בין הסגמנטים השונים באמצעות הפרדה פיזית או לוגית של הרשת, הגבלת אפשריות הקישוריות בין הרשתות השונות והקמת סביבה מבוקרת באמצעות חומת אש, ו/או רכיב תכנה (מיקרו סגמנטציה) שיואשר ע"י אגף הסייבר וזאת בהתאם לפעילויות הנדרשות מהמערכת, לפרוטוקולים, לכתובות ול- ACL'S.

3.10.4 כל העברת מידע לרשת רכבת ישראל תבוצע לאחר בחינה ואישור של אגף הסייבר ברכבת ישראל, ובכל מקרה לאחר סינון תוכן/שבירת פרוטוקול.

3.10.5 תבוצע הפרדה של סביבות עבודה ע"פ חלוקה ל- ייצור, טסט ופיתוח.

3.10.6 תבוצע הפרדה לתתי רשתות כגון: שרתי אפליקציה, בסיס נתונים ודוחות.

3.10.7 הספק נדרש ליישום תהליך מאובטח להעברת מידע מסביבה לסביבה, לרבות תמיכה ב-workflows מתאימים לנושא.

3.10.8 הספק נדרש ליישם יכולת Scrambling לנתונים רגישים במעבר מסביבת הייצור לסביבות אחרות כדי שלא יופיעו בסביבות הלא מבצעיות (Test, QA וכו') "as is".

## 3.11 בקרת גישה- דרישות חובה

3.11.1 הגישה לסביבת המידע של רכבת ישראל תחייב הזדהות של המשתמש ותוגבל לבעלי צורך עסקי בלבד.

3.11.2 הרשאות המשתמש יוקצו בהתאם לצורך העסקי ולפי עקרונות "הצורך לדעת" ("need to know") ו"מינימום הרשאות" ("Least Privilege"). בשיטה זו יוגדרו הרשאות ספציפיות לאובייקטים במערכת, על-פי שמות המשתמשים, שמות קבוצות משתמשים, או שניהם יחד. שינוי הרשאות הגישה יתבצע על-ידי גורמים מוסמכים בלבד.

3.11.3 חשבונות משתמש בעלי הרשאות חזקות (למשל: מנהל מערכת) יוקצו למספר המינימלי הנדרש של עובדים.

3.11.4 לכל מורשה גישה לסביבת המידע של רכבת ישראל יוקצה מזהה משתמש (user ID) ייחודי. השימוש בחשבון קבוצתי או חשבון משותף בסביבת המידע של רכבת ישראל אסור.

3.11.5 חשבונות של עובדים שעזבו או החליפו תפקיד ואינם קשורים עוד לשירותים עבור רכבת ישראל, ייחסמו או יבוטלו.

3.11.6 חשבונות אפליקטיביים- יוגדרו בנפרד מחשבונות משתמשי מערכת, וזאת לאחר אישור אגף הסייבר ברכבת ישראל.

## 3.12 מדיניות סיסמאות- דרישות חובה

3.12.1 הספק יאכוף מדיניות של סיסמאות חזקות:

3.12.2 אורך סיסמה יהיה 8 תווים לפחות.

3.12.3 הסיסמה תהיה מורכבת משילוב של אותיות גדולות, אותיות קטנות, ספרות וסמלים, לפחות אות אחת גדולה, 2 מספרים וסמל מיוחד אחד.

3.12.4 אורך סיסמא למשתמש חזק (Admin) יהיה 12 תווים לפחות ויחייב הזדהות בשני אמצעים (Two-Factor authentication). למשל: סיסמת משתמש + OTP

3.12.5 הסיסמה למשתמש חזק (Admin) תהיה מורכבת משילוב של אותיות גדולות, אותיות קטנות, ספרות וסמלים, לפחות אות אחת גדולה, 2 מספרים וסמל מיוחד אחד.

3.12.6 תתבצע אכיפה של החלפת סיסמה ראשונית (שסופקה ע"י מנהל רשת/מערכת) בסיסמה קבועה, מיד לאחר הזדהות הראשונה למערכת.

3.12.7 תתבצע אכיפה של החלפת סיסמה כל 3 חודשים לפחות. משתמש לא יוכל לבחור סיסמה חדשה הזהה לאחת מחמשת הסיסמאות האחרונות שלו.

3.12.8 תיושם הגנה קריפטוגרפית על סיסמאות, הן באחסון והן בתעבורה. שיטת ההגנה תהלום את ההמלצות העדכניות בתחום.

3.12.9 חיבור מערכת (session) שאינו פעילת במשך 20 דקות, ינותק באופן אוטומטי. חידוש החיבור ידרוש מהמשתמש הזדהות חוזרת.

3.12.10 חשבון משתמש יינעל לאחר 5 ניסיונות גישה כושלים. שחרור הנעילה יתאפשר רק אחרי 30 דקות לפחות, או על-ידי מנהל המערכת, לאחר תהליך אימות של זהות השתמש.

3.12.11 בכל התחברות בגישה מרחוק (remote access/מערכות תקשוב) לסביבת המידע של רכבת ישראל תתבצע בערוץ מוצפן (למשל: ssl-vpn/ httsp) ותחייב הזדהות בשני אמצעים (Two-Factor authentication). למשל: סיסמת משתמש + OTP.

## 3.13 <u>אבטחת שרתים ותחנות קצה- דרישות חובה</u>

3.13.1 ככלל, כלל מערכות ההפעלה והתוכנות בשימוש יהיו תחת תמיכה ועדכונים של היצרנים.

3.13.2 הספק יקשיח ויגדיר את כל השרתים ותחנות הקצה אשר בסביבת המידע של רכבת ישראל, בהתאם להוראות היצרנים או להמלצות המקובלות בתחום (Best Practices) כגון: CIS

3.13.3 יישומים, שירותים, פורטים, מודולים, רכיבים וכדומה שאינם נחוצים לפעילות ולשימושים העסקיים שהוגדרו, ייחסמו או יבוטלו.

3.13.4 כל החשבונות וסיסמאות ברירת המחדל של היצרן בכל הרכיבים בסביבת המידע של רכבת ישראל (מערכת הפעלה, רכיבי תוכנה, רכיבי תקשורת וכדומה), יוסרו או ייחסמו ובמקומם יוגדרו חשבונות ייעודים של הספק עם סיסמאות חזקות.

3.13.5 עדכוני אבטחה קריטיים לרכיבי תוכנה ומערכות הפעלה בסביבת המידע של רכבת ישראל, יותקנו בסמוך ככל האפשר למועד פרסומם ע"י היצרנים, ולכל היותר תוך 30 יום. עדכונים שאינם קריטיים יותקנו אחת לרבעון.

3.13.6 כלים אוטומטיים להגנה מפני תוכנות זדוניות (לדוגמא: אנטי וירוס ו-EDR) יותקנו בכל השרתים ותחנות הקצה בסביבת המידע של רכבת ישראל. הספק יוודא עדכניות כלים אלה בכל עת.

3.13.7 ייושמו בקרה והגבלה על התקנת תוכנות בתחנות הקצה הקשורות לסביבת המידע של רכבת ישראל (Application Control).

3.13.8 תיחסם תכונת ההפעלה האוטומטית (Auto-run) בשרתים ובתחנות הקצה.

3.13.9 בתחנות הקצה יופעל Personal Firewall, בקרות קונפיגורציה ותכונות נשלטים ומנוהלים מרכזית ובאחריות הספק.

## 3.14 <u>פיתוח מאובטח- דרישות חובה</u>

3.14.1 הספק יתחייב כי הינו מיישם עקרונות פיתוח מאובטח הנותן מענה לחשיפות של owasp top 20.

3.14.2 הספק ימלא אחר עקרונות פיתוח מאובטח כגון: אימות קלט, אימות פלט, ניהול סיסמאות ואישור, ניהול sessions, בקרת גישה והרשאות,

הצפנת נתונים, טיפול ביומן וביקורת תקלות, הגנת נתונים, תקשורת מאובטחת, תצורת שרת והקשחה.

3.14.3 בעת שימוש בקוד צג ג', נדרש לקבל את אישורו של הספק בכתב על גבי מסמך עם לוגו החברה וחתום ע"י מנכ"ל, כי הקוד על כל מרכיבי נבדק ע"י החברה ונמצא ללא חשיפות/פגיעויות שעלולים להשפיע על תקינות מערכות ורשת הרכבת, בנוסף, יידרש הספק להעביר לרכבת ישראל דו"ח מרכיבי SBOM, לא יאושרו רכיבים לשימוש עם פגיעויות ברמה בינונית ומעלה.

3.14.4 טרם עלייה לאוויר, יערך סקר אבטחת מידע ומבדק חוסן על ידי חברה צד ג' המתמחה בביצוע סקרים ומבחני חדירה, ע"פ מתודולוגית מקובלות. תכולת סקר ומבדק החדירה יעבור לאישור של אגף הסייבר ברכבת ישראל.

3.14.5 הספק יידרש לתקן ליקויים שעלו בסקר אבטחת המידע ומבדק החוסן ברמת חומרה גבוהה/בינונית על חשבונו ובהתאם להנחיות של אגף הסייבר ברכבת ישראל.

3.14.6 הספק יתחייב לבצע כל שנה קלנדרית מבחני חדירה למערכת על ידי חברה צד ג' **המתמחה בביצוע מבחני PT**, תוצאות המבדק יועברו ויאשרו כי אין למערכת ליקויים ברמות סיכון גבוהה ובינונית.

3.14.7 הדוח הסופי שיוגש לאגף הסייבר יכיל את הנתונים הבאים:

3.14.7.1. "תמצית מנהלים" המכילה פרטים כלליים על המערכת (תיאור, ארכיטקטורה, היקף הבדיקה ומגבלותיה), סיכום ממצאים ביחס לחשיפה האבטחתית וביחס לתאימות לחוזרים בנושא אבטחת מידע החלים על המערכת, פירוט הממצאים.

3.14.7.2. סיכום הממצאים יתבצע לפי הפורמט להלן:

| מספר | סעיף בדו"ח | רמת הסיכון | תיאור כללי | המלצה לטיפול |
|---|---|---|---|---|
| ID הקיים בטבלת המעקב | | | | |

3.14.8 פירוט הממצאים יכיל את הנתונים הבאים: הנושא הנבחן, תיאור הבדיקה, ממצאי הבדיקה, תיאור החשיפה, רמת סיכון (סבירות התרחשות, פוטנציאל נזק), המלצות ישימות או בקרות מפצות, פירוט טכני – הסבר מדויק (כולל צילומי מסך ו/או הקלטה) כיצד גילו את הממצא, כדי שניתן יהיה לשחזר לבד את הממצא. במידה והממצא הינו ממצא פתוח מסקר קודם נדרש לציין זאת בדו"ח.

3.14.9 דו"ח סקר יהווה מסמך מנחה לביצוע פעולות אופרטיביות. הדו"ח יפרט את הממצאים ורמת הסיכון המבוססת על הסבירות מול הנזק של כל חשיפה כמו גם המלצות לטיפול בליקויים על פי תעדוף.

3.14.10 פירוט הממצאים המפורט לעיל תקף הן לממצאים הקודמים והן לחדשים.

## 3.15 <u>שימוש במדיה נתיקה- דרישות חובה</u>

3.15.1 בסביבת המידע של רכבת ישראל יותר שימוש אך ורק במדיה נתיקה שעברה תהליך של "הלבנה" (סריקה וסינון של קבצים, טרם הכנסתם לסביבת המידע) וזאת לאחר אישור אגף הסייבר ברכבת ישראל.

3.15.2 מדיה נתיקה המכילה מידע של רכבת ישראל שסווג כחסוי, תוצפן בהתאם לסטנדרטים המקובלים בתחום.

## 3.16 **תחזוקה- דרישות חובה**

3.16.1 פעילויות יזומות (לרבות: שדרוג, הרחבה) יבוצעו בתיאום ועל פי מדיניות רכבת ישראל - לאחר קיום ישיבות מתועדות בהן ידונו משמעויות הפעילויות, כגון: וידוא מוכנות, דיון בנושא חזרה לאחור, קבלת אישורים, תקשור משמעויות, מניעת סיכונים לרציפות השירות וכו'.

3.16.2 ככלל, גישה לשרתי רכבת ישראל לצורך פעילויות תחזוקה תתבצע במתקני רכבת ישראל בלבד. לא תתאפשר גישה מרוחקת לשרתים, או לחלקי המערכת. כל החרגה מסעיף זה תאושר פרטנית ע"י מנהל אגף הסייבר ברכבת ישראל.

3.16.3 עדכונים ושינויים לתוכנה/תשתית - כל שינוי במערכת (למעט עדכון תוכן) מהווה "גרסה" ועליה לעבור בדיקות בהתאם לדרישות רכבת ישראל. (כגון: בדיקות חדירות, סקר קוד וכו').

3.16.4 בהתאם להנחיות הרכבת ועל פי לוח הזמנים שיינתן לו, הספק יציג פתרון למניעת גישה למרכיבי מערכת במסגרת מתן התחזוקה למערכת, להגנתה ולבקרתה.

## 3.17 **הצפנה- דרישות חובה**

3.17.1 כל תעבורה רשתית מחויבת בהצפנה עצמאית (אלגוריתם מזערי מחייב ביסוס על תקן AES256, ומעלה), וללא תלות בהצפנה רשתית.

3.17.2 כל מידע הנשמר במערכת מחויב בהצפנה עצמאית (אלגוריתם מזערי מחייב ביסוס על תקן AES256, ומעלה), וללא תלות בהצפנה רשתית.

3.17.3 כל התעבורה תהיה מוצפנת בפרוטוקולי הצפנה מסחריים, כגון: IPsec, TLS/SSL, SSH וכו'.

3.17.4 על המערכת לתמוך בתקן הצפנה FIPS[3] 140-2.

3.17.5 חריגה ממדיניות ההצפנה תייצר רשומה הניתנת להעברה ממוכנת ומקוונת להיררכיית ניטור, בפורמט המוכר והמותאם למערכות ה-SIEM המותקנות ברכבת ישראל, וזאת לאחר אישור אגף הסייבר ברכבת ישראל.

3.17.6 בעת רכש מחשבי תחנות קצה (נייחים, או ניידים) לפרויקט, יש לוודא כי המוצר מכיל רכיב TPM (Trusted Platform Module) מובנה, המאפשר הצפנת דיסקים.

## 3.18 **ניטור, לוגים ובקרה-דרישות חובה**

[3] Federal Information Processing Standards

3.18.1 כלל הלוגים יועברו למערכת SIEM מרכזית, מטרת המערכת הינה איסוף הלוגים והגנה עליהם. בנוסף, למערכת ה- SIEM תהיה יכולת לביצוע קורלציה לזיהוי ותחקור אירועי סייבר.

3.18.2 הרכיבים הבאים לפחות ירשמו לוג אירועים: מערכות ההפעלה של השרתים, אפליקציות השירות, מנגנוני אבטחה (Active Directory (Firewall, IPS/IDS WAf, Web Proxy Anti virus, EDR,PSM,PIM

3.18.3 כל פעולה עסקית במערכת, תחויב ביצירת רשומת לוג, וכמו כן תאפשר יישום מנגנון מעקב ומניעת התקשחות.

3.18.4 קבצי החיווי (לוגים) יהיו זמינים לבחינת נציג רכבת ישראל בכל עת וללא כל עלות/חיוב נוסף.

3.18.5 הספק יתחייב להמציא לרכבת ישראל כל ראיה בהקשר זה (דיגיטלית, כתובה או אחרת) תוך 48 שעות ממועד הבקשה.

3.18.6 כל פעולה חייבת להיות מתועדת ברשומה אבטחתית. יתאפשר קישור תוצרי הניטור והלוגים (הרלוונטיים להתקשרות) ממערכות הספק למרכז הניטור הקיברנטי של רכבת ישראל תוך התממשקות למערכת ניהול האירועים (SIEM) של רכבת ישראל.

3.18.7 המערכת תאפשר יכולת העברת קבצי חיווי ל-SIEM בהתאם לסטנדרטים מקובלים כגון Syslog.

3.18.8 הספק יאפשר תמיכה בהתממשקות למרכז הניטור הקיברנטי ע"י רכיב תקשורת חד כיווני- דיודה.

3.18.9 להלן פעולות הבקרה המהוות דרישות מנדטוריות ליישום וניטור במערכת:

3.18.9.1. תיעוד של כל ניסיונות הגישה למערכת ולמסד הנתונים, לרבות גישה מחשבונות ניהול (Administrator), תמיכה, DBA, System ,Audit;

3.18.9.2. התנתקות מהמערכת;

3.18.9.3. הרשאת גישה וניטור בעת גישה למסד הנתונים בסביבת הייצור (Production) תוגדר בלעדית למנהל המערכת ולגורמים באישורו-כל אחד בחשבון אישי ובלעדי;

3.18.9.4. חסימת וניטור חשבון גישה למאגר הנתונים-לאחר 5 הזדהויות שגויות;

3.18.9.5. הפקת דו"ח כשלים בהליכי הזדהות, או בניסיונות גישה בלתי חוקיים ברמת מערכת ההפעלה ומסד הנתונים;

3.18.9.6. ניטור כל שינוי, או מחיקת אובייקטים במערכת;

3.18.9.7. ניטור וחסימת כל שינוי (לרבות מחיקה) בתכנה, בטבלאות, בנתונים ובבקרות של מסדי הנתונים;

3.18.9.8. ניטור אירועים אפליקטיביים שיוגדרו כדורשי בקרה עפ"י מנגנון כללים מיוחד לנושא;

3.18.9.9. ניטור התחלת פעילות מסוימת אשר תוגדר כדורשת בקרה ע"י המשתמש (כגון: פתיחת כספת, שליחת מסר וכו');

3.18.9.10. ניטור ביצוע פעילויות המבוצעות על-ידי גורמים בעלי הרשאות גבוהות;

3.18.9.11. ניטור פעולות אדמיניסטרציה (ניהול משתמשים, הורדה והעלאת מערכת, services, וכו');

3.18.9.12. ניטור שגיאות תפעוליות (נפילת מערכת, הודעות שגיאות תוכנה, וכו');

3.18.10 עבור כל אירוע המוגדר כדורש בקרה יישמרו הפרטים הבאים:

3.18.10.1. תאריך ושעה;

3.18.10.2. מקור ביצוע הפעולה (דוגמא: כתובת IP, domain);

3.18.10.3. שם המשתמש;

3.18.10.4. סוג האירוע;

3.18.10.5. הצלחה, או כישלון של האירוע;

3.18.10.6. זיהוי האובייקט עליו מבוצעת הפעולה (שם קובץ וכו');

3.18.10.7. תיאור הפעולה (מה בוצע?): עבור כל סוג אירוע יש לספק תוכן רלוונטי. למשל: עדכון רשומה, ניסיון גישה לרשומה, מחיקת משתמש, הורדת מערכת, וכו;

3.18.11 המערכת תתמוך בהצגה וניתוח של מגמות ושימושים (Trends &Usage) לאורך זמן.

3.18.12 המערכת תאפשר "להעשיר" את המידע בלוג, לרבות: סוג המכונה, סוג מערכת ההפעלה, User Agent וכיו"ב.

3.18.13 ההודעות צריכות להיות אמינות, מלאות וברורות. קבצי החיווי (לוג) במערכת יהיו מוגנים מפני גישה (צפייה, שינוי, מחיקה) לא מורשית, לרבות משתמשים בעלי הרשאות ניהול ותישמר האפשרות לזהות גישה לא מורשית.

3.18.14 המערכת תתריע על ניסיון גישה/שימוש, החורג מגבולות ההרשאות שניתנו.

3.18.15 על המערכת לנהל תהליך מובנה וסדור של אחסון ומחיקת רשומות.

3.18.16 רשומות הלוג תישמרנה למשך 6 חודשים לפחות.

3.18.17 למערכת תהיה יכולות דיווח (בדוא"ל SMS, SNMP, TRAPS וכו') למנהלי המערכת על אירועים שיוגדרו כדורשי דיווח.

3.18.18 על מערך הבקרה להיות מאובטח כיאות. רק משתמשים מורשים יקבלו גישה אליו, ובמיוחד יש להקפיד על בקרת גישה ליכולת להעלות ולהוריד את מנגנון הבקרה.

3.18.19 המידע אשר ישמר בקבצי החיווי יעמוד בדרישות תקן אבטחת מידע בסקטור כרטיסי האשראי (PCI-DSS) ו/או בתקנות הרשות להגנת הפרטיות, ככל שרלוונטי לנושא.

3.19 **<u>טיפול ומוכנות לאירועי סייבר ואבטחת מידע- דרישות חובה</u>**

3.19.1 על הספק להכין תכנית היערכות ותגובה לאירועי אבטחת מידע וסייבר (Incident Response Policy and Procedure).

3.19.2 במסגרת התוכנית, הספק יגדיר תכנית הכוללת היערכות, זיהוי, בלימה, מיתון, שחזור (BCP) ויעדי התאוששות מאירוע אבטחת סייבר עד לתפקוד מלא בעת חזרה לשגרה.

3.19.3 מקום בו תעלה דרישה, הספק יציג לאגף הסייבר ברכבת ישראל את עקרונות התוכנית והתאמה להערכת הסיכונים שבוצעה.

3.20 **<u>ביצוע סקרים, שרשרת אספקה-דרישות חובה</u>**

3.20.1 הספק מתחייב לעמוד ברף "רמת סיכון מהותית" לשאלון שרשרת האספקה של מערך הסייבר הלאומי, וזאת ע"פ הקטגוריה הרלוונטית (לדוגמא, מחשבון ענן, Hosting, ניהול אבטחת מידע וכדומה).

3.20.2 בהתאם לנספח זה, רשאית הרכבת לערוך סקר סיכונים, או באמצעות צד ג' ללא כל עלות נוספת.

3.20.3 הספק מתחייב לאפשר לנציגי הרכבת לבצע ביקורת מערכי אבטחה, במשך שעות העבודה המקובלות וללא התראה מוקדמת, במתקניו, אשר להם זיקה, או השפעה על אבטחת המערכות המשמשות את רכבת ישראל ללא כל עלות נוספת.

3.20.4 הרכבת, או נציגיה המוסמכים, יהיו רשאים לבצע בדיקות מערכי אבטחה, בקרת חסינות, איתור פרצות אבטחה ובדיקת יעילותם של מנגנונים המשמשים לאבטחת המערכות המשמשות את רכבת ישראל ללא כל עלות נוספת.

3.20.5 על הספק לערוך בדיקות אבטחה סמויות ממערכים חיצוניים לספק, לבדיקת ההגנות בפני גישה חיצונית ממערכות הספק, או ממערכות חיצוניות לספק, אל מערכות רכבת ישראל, נשוא ההתקשרות.

3.20.6 רמת הכיסוי של הסקרים תותאם לרגישות המידע ולרמת הסיכון הנשקף לרכבת ישראל, מאופי הפעילות מול הספק ותכלול בדיקות שמטרתן לוודא את עמידת הספק בדרישות הגנת סייבר ולזהות חשיפות לסיכונים אלו.

3.20.7 רכבת ישראל רשאית לדרוש תיקון ליקויים, אשר יתגלו בסקרי סיכונים, ביקורות מתוכננות, ביקורות פתע, גילוי אקראי, או יזום של ליקויי אבטחה במתקני הספק- והספק יחויב לתקן ליקויים אלו, תוך פרק זמן סביר (לעניין זה - הזמן המוערך ע"י גופים מקצועיים לתיקון הליקוי) וללא כל עלות נוספת.

3.20.8 במידה וימצאו ליקויים קריטיים המשפיעים על רמת הגנת הסייבר של מערכות רכבת ישראל, יידרש הספק לתקן ליקויים אלו באופן מיידי וללא כל עלות נוספת.

3.21 **<u>דו"חות בקרה-דרישות חובה</u>**

3.21.1 הספק מתחייב להעביר לרכבת ישראל לפי דרישה, או בהליך שוטף דו"חות בקרה, אשר נדרשו במסמכי ההתקשרות ודו"חות נוספים

על-פי הצעתו של הספק, ללא חיוב נוסף. בין הדו"חות יכללו:

3.21.1.1. דו"חות על מערכת ההרשאות (הרשאות למשתמש, משתמשים בקבוצת משתמשים, וכו')

3.21.1.2. דוחות ממערכת הניטור (Auditing), לרבות: מספר אירועים מכל סוג, ניסיונות גישה כושלים, וכו'.

3.21.2 קבצי הדוחות יתאימו ככל הניתן לתוכנות חיצוניות אחרות ובפורמטים מקובלים כגון XML, Doc, TXT, וכו'.

3.21.3 הדו"ח יכלול Banner המסווג את הדו"ח, יציין את שם המשתמש שהפיק אותו וכן יציין נתוני תאריך ושעה.

3.21.4 הדו"חות יועברו לרכבת ישראל כשהם ממוינים על-פי הנתונים, שידרשו מהספק.

## 3.22 <u>גישה מרחוק-דרישות חובה</u>

3.22.1 ככלל, לא תתאפשר לספק כל גישה מרחוק למערכות רכבת ישראל.

3.22.2 על אף האמור בתתי הסעיפים לעיל, תותר הקמת תווך בין מתחמי הספק לבין רכיבים ממערכות רכבת ישראל, רק אם יתקיימו התנאים הבאים:

3.22.2.1. החיבור יבוצע אך ורק ממחשבי קצה שהספק יעביר לרכבת ישראל, מחשבים אלו יוקשחו ע"י רכבת ישראל.

3.22.2.2. הקמת התווך נבחנה ואושרה על ידי אגף הסייבר ברכבת ישראל, לאחר שנבחן הצורך/הכורח שבהקמת התווך, נבחנו הסיכונים שבהקמת התווך והבקרות המפצות.

3.22.2.3. הגישה מרחוק תהיה מוגבלת רק לרכיבים אליהם קיימת חובת התחברות מרחוק.

3.22.2.4. הגישה מרחוק תהיה מוצפנת (בהתאם לדרישות המצוינות בסעיף "הצפנה")

3.22.2.5. יוגדרו פרקי זמן של חוסר פעילות שלאחריהם תתנתק הגישה (Session Timeout).

3.22.2.6. גישה מרחוק תבוקר ותוגבל לעובדים של הספק אשר יאושרו ע"י רכבת ישראל מראש, כאשר לכל עובד יהיה שם משתמש אישי. היה ולא ניתן להגדיר שם משתמש אישי, יוגבלו הרשאותיו של המשתמש הקבוצתי לפעולות של ניטור ואתחול בלבד ולא תותר כל התקנה, או עדכון של רכיב תוכנה-באמצעות גישה מרחוק.

## 3.23 <u>חומרה- דרישות חובה</u>

3.23.1 בכל רכש המיועד לרשתות, אמצעי הגנה (מסוג חומרה ותכונה) תשתית מערכות חיוניות, ומערכות הבקרה התעשייתיות ברכבת ישראל, יהיו כפופים לאישור אגף הסייבר ברכבת ישראל.

3.23.2 בעת רכש שרתים ותחנות קצה (נייחים, או ניידים) לפרויקט באחריות הספק לוודא כי:

3.23.2.1. שרתים ותחנות קצה נייחות לא יכילו רכיב תקשורת אלחוטי מובנה, לרבות:

WIFI, Bluetooth, InfraRed וכו'.

3.23.2.2. המוצר יכלול רכיב TPM מובנה המאפשר הצפנת דיסקים. (ראה סעיף **Error! Reference source not found.** לעיל.)

3.23.2.3. אמצעי האחסון של המוצר יהיו אמצעים פנימיים בלבד, ללא שימוש בדיסקים קשיחים נשלפים.

3.24 **<u>קניין רוחני- דרישות חובה</u>**

3.24.1 כל התוכנות ומערכות המחשוב אשר משמשות את הספק במתן השירותים לרכבת ישראל, עומדות בדרישות הדין בתחום הקניין הרוחני, רישיונן תקף ולספק זכות שימוש בהן.

3.24.2 לא יעשה שימוש בתוכנות וציוד אשר אינם נתמכים עוד על ידי היצרן ואשר הוגדרו על ידו כ- End Of Life.

3.25 **<u>מחשוב ענן</u>**
**<u>דרישות כלליות למחשוב ענן</u>**

3.25.1 סיווג הנתונים המאושר לשימוש במחשוב ענן הוא עד סיווג בלמ"ס עד וכולל, כל מידע בסיווג שונה דורש אישור פרטני של אגף הסייבר ברכבת ישראל.

3.25.2 מעבר לכל המפורט במסמכי ההתקשרות ו/או נספחים אחרים, על תהליכי העבודה של הספק להבטיח שמירה על כל מרכיבי אבטחת המידע (חסיון המידע, תקינות/שלמות המידע ורציפות השירות).

3.25.3 על ספק שירות הענן לספק לפי דרישה תיעוד של כל היכולות הנדרשות ממנו במסמך דרישות זה והמשמשות אותו בהפעלת שירות הענן - ובכלל זה יכולות אמצעי וכלי הניטור, התיעוד, החישוב, האחסון, בקרת גישה, ניהול זכויות גישה, עקיפת מנגנוני הפעלה ואבטחה, הצפנה (קריפטוגרפיה) ואחרות.

**<u>דרישות חובה- מחשוב ענן</u>**

3.25.4 בהתאם ללוח הזמנים והנחיות נוספות שיקבל מנציגי הרכבת, הספק יעביר תכנון HLD הכולל את תצורת המערכת, תיאור סביבות העבודה (ענן ציבורי, ענן פרטי, ענן היברידי), תוך ציון מודל פריסת שירותי הענן (SaaS,IaaS,PaaS), קיום מודל אחריות משותפת (Model Responsibility Shared) וכן מיפוי זרימת הנתונים בין כלל שירותי הענן לבין מערכות מחשוב הפנימיות ברכבת ובין כל הלקוחות/צמתים אחרים.

3.25.5 בהתאם ללוח הזמנים והנחיות נוספות שיקבל מנציגי הרכבת, הספק יעביר תוכנית LLD הכוללת תכנון ארכיטקטורה מעמיק,

רשימות ציוד ויצרנים, אפיון מפורט של הממשקים ותוכנית המימוש.

3.25.6 על הספק לעמוד בכל דרישות החובה של אגף הסייבר ברכבת ישראל כפי שפורט מעלה, החל מסעיף 3.1 ועד לסעיף 3.24, בעת אספקת שירותים בתשתיות ענן.

3.25.7 על הספק לעמוד ברף "רמת סיכון מהותית" לשאלון שרשרת האספקה של מערך הסייבר הלאומי.

3.25.8 מחשוב ענן יתבצע בתשתיות מחשוב ענן העומדות בתקני הענן המובילים כגון: (לפחות 2 מתוך 5 תקנים בינלאומיים).

3.25.8.1. CSA STAR;

3.25.8.2. SOC2;

3.25.8.3. IEC 27017;

3.25.8.4. IEC 27018;

3.25.8.5. FedRAMP;

3.25.9 הספק נדרש לעמידה מלאה של השירות בענן בחוק הגנת הפרטיות תשמ"א- 1981, על התקנות שהותקנו מכוחו, לרבות תקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), תשס"א-2001, בנושא העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה.

3.25.10 ככל ורלוונטי, הספק נדרש לעמידה מלאה ברגולציית ה- Privacy Shield וה- GDPR המטפלות בשמירה על פרטיות במידע.

3.25.11 ככל ורלוונטי, הספק נדרש לעמידה מלאה בתקן PCI-DSS-Cloud Computing Guidelines.

3.25.12 ככלל, תצורת המידור של הגישה לסביבת המידע של רכבת ישראל, גם בעת פעילות תקינה וגם בעת עלייה מכשל או שחזור מידע תוגדר באמצעות הפרדה ל- Tenant שישרת את שירותי/משאבי החברה בלבד.

3.25.13 הספק יעשה שימוש בפתרון Cloud security access brokers CASB לשם מענה לסיכונים בשירותי ענן, אכיפת מדיניות אבטחה ועמידה בדרישות רגולציה, גם כאשר שירותי הענן חיצוניים לאתר הספק ומחוץ לשליטה הישירה של הספק.

3.25.14 ככלל, סביבת המידע של רכבת ישראל המאוחסנת בשירותי ענן, תהיה מוצפנת על ידי אמצעי הצפנה מקובלים, כאשר מפתח ההצפנה ישמר מחוץ לשירותי הענן באמצעות כספת לוגית.

3.25.15 בכל גישה לניהול/צריכת שירות בענן, תופעל הזדהות חזקה וזאת באמצעות MAF- Multi Factor Authentication.

3.25.16 הספק נדרש לבצע בקרת גישה תקשורתית לממשקי הניהול של השירות בענן.

3.25.17 הספק נדרש לבצע בקרה ויכולת מניעה של מנהלים מטעם הספק לסביבת המידע של רכבת ישראל המאוכסן בענן.

3.25.18 קישור וממשקים לרשת רכבת ישאל יבוצעו לאחר בחינה ואישור של אגף הסייבר ברכבת ישראל, ובלבד שיבוצעו ע"י הצפנת תווך בלבד.

3.25.19 העברת מידע לרשת רכבת ישראל תבוצע לאחר בחינה ואישור של אגף הסייבר ברכבת ישראל, ובכל מקרה לאחר סינון תוכן/שבירת פרוטוקול.

3.25.20 יופעל תנאי גישה Conditional Access, כך שהשירות המסופק יהיה זמין מכתובות רכבת ישראל בלבד.

3.25.21 במידה ונדרש שירות זמין לשימוש חיצוני, תוגבל רשימת כתובות ה-IP (GEP) למדינות אויב או עפ"י רשימה שאגף הסייבר יעביר.

3.25.22 תהליכי העבודה של הספק בשירות ענן יבטיחו בקרה, ניטור ותיעוד הגישה לסביבת המידע השייך לרכבת ישראל, תוך מניעת ותיעוד כל גישה בלתי מורשית וניסיון גישה מצד בלתי מורשים אל המידע (ובכלל זה ניסיונות יצירת עותקים של המידע – מגנטיים או מודפסים), והתרעה לרכבת ישראל על כל גישה בלתי מורשית, או ניסיון לכך.

3.25.23 תהליכי העבודה של הספק בשירות ענן יבטיחו הגנה על קבצי חיווי (Audit) ונתונים אחרים (לרבות: מצבי מערכת ופעולות אשר בוצעו כתגובה) הנדרשים לצורך ניתוח אירועי כשל בכלל ואירועי סייבר בפרט.

3.25.24 על מערכות הניטור של הספק לזהות אירועי אבטחת מידע ולהתריע לרכבת ישראל בטווחי זמן אפקטיביים וזאת במטרה לעמוד ביעדי הזמן הנדרש לטיפול באירועים ולנטרל את איומי אבטחת המידע בשירותי ענן מוקדם ככל האפשר ובאופן יעיל ומהיר ולמנוע כל סיכון למידע, או לשירות הקיים בענן.

3.25.25 מערכות הניטור בענן יאפשרו לכל לקוח גישה לחיוויים אודות מערכותיו בלבד. לא תתאפשר גישה לחיוויים אודות מערכות רכבת ישראל לגורמים אחרים ללא קבלת אישור רשמי מאגף הסייבר ברכבת ישראל, טרם מתן הגישה.

3.25.26 כלל אירועי אבטחת הסייבר של תשתית/כל שירות אחר בענן ישמרו בלוג אירועים לפחות לתקופה של חצי שנה.

3.25.27 יתאפשר קישור תוצרי הניטור והלוגים (הרלוונטיים להתקשרות) ממערכות הספק למרכז הניטור הקיברנטי של רכבת ישראל תוך התממשקות למערכת ניהול האירועים (SIEM) של רכבת ישראל.

3.25.28 על הספק להגדיר תהליכים יעילים ומהירים לטיפול בתקלות בשירות/מערכת הקיימים בענן ובכלל זה מענה מהיר, יעיל ורציף לפניות ודיווחים אודות תקלות כאלו (כגון מוקד זמין לתמיכה ושירות). לצורך הבטחת רציפות המענה על הספק לקיים מנגנונים אשר ימנעו את חסימת והשבתת שירות מוקד התמיכה.

3.25.29 על הספק להבטיח את רציפות השירות הקיים בענן ובין היתר תוך ניטור הקצאת המשאבים (זיכרון, עיבוד, תקשורת) וקיום מנגנוני התאוששות מאסון, ובכלל זה קיום אתר שעון והסתמכות על תהליכים וגיבויים (ובכלל זה אחסון באתרים פיזיים שונים) המאפשרים ומבטיחים שחזור מהיר.

3.25.30 **<u>הסרת שירות ענן-דרישות חובה</u>**

3.25.30.1. לצורך הסרת שירות ענן (בהתאם לתנאי ההתקשרות בכלל ועם תום ההתקשרות בפרט) על ספק שירות הענן למחוק

את כל המידע השייך לרכבת ישראל והקיים בשירות הענן ובכלל זה את "המידע-אודות-המידע" (Meta-Data), תוך הסרת כל אפשרות לשחזור המידע.

3.25.30.2. טרם מחיקת המידע המפורט בסעיף הקודם לעיל, על ספק שירות הענן לקבל את אישור רכבת ישראל למחיקת המידע ולהעביר לרכבת ישראל גיבוי מלא ושלם של כל המידע השייך לרכבת ישראל ולפרויקט/מערכת.

## 4. תצורת המערכת

4.1 במידה והמערכת מכילה מידע **פנימי/רגיש אישי/רגיש עסקי**, המערכת תותקן בחוות השרתים ברכבת ישראל (On premise) וזאת לאחר אישור אגף הסייבר ברכבת ישראל טרם התקנתה.

4.2 לחלופין, בהתאם להנחיות ולאחר אישור אגף הסייבר ברכבת ישראל, המערכת יכולה להיות מסופקת בתצורת "ענן" לאחר בחינה פרטנית של אגף הסייבר ברכבת ישראל.

4.3 המערכת תתמוך בכל הדרישות על פי נספח זה, בין אם התקנת המערכת היא בתצורת On premise ובין אם אספקת המערכת והשירותים היא בתצורת ענן.

4.4 תצורת התקנת המערכת תאושר ע"י אגף הסייבר ברכבת ישראל, וזאת לאחר שנבחנו ואושרו ארכיטקטורות HLD ו-LLD שהעביר הספק.

4.5 במידה ומדובר ביישום של תצורת ענן, הרי שהספק יידרש לענות על מכלול דרישות אבטחת מידע בנספח זה בסעיף מחשוב ענן לעיל.

4.6 הספק יתקין את המערכת, וכן יגדיר הגדרות, בהתאם להנחיות בנספח זה ובהתאם להנחיות רכבת ישראל, וישלב אותה באתרי רכבת ישראל, על בסיס תשתית התקשורת והמערכות הקיימות והפועלות בכל אתר ואתר, עד לתפעול מלא ותקין בסביבת הייצור.

4.7 מימוש המערכת יכלול התממשקות למערכות רכבת ישראל באמצעות ממשק מכונה (API) לייצוא וייבוא נתונים, לאחר בחינה, אישור ובהתאם לדרישות והנחיות אגף הסייבר ברכבת ישראל.

## 5. ביטחון ואבטחה פיזית

5.1 הספק ימלא את כל דרישות הרכבת בנוגע לאבטחת מידע, לרבות דרישות פרטניות לאבטחה פיזית, אבטחת סביבת מחשוב, הגנה על מסמכים וציוד במתקניו ולתהליכי בדיקות מהימנות לעובדיו.

5.2 הגישה הפיזית לסביבת המידע של רכבת ישראל תוגבל לבעלי צורך עסקי בלבד. הסביבה תהיה מוגנת מפני גישה של גורמים בלתי מורשים באמצעות מערכות בקרת גישה וכניסה.

5.3 כל הרכיבים וההתקנים בהם מאוחסן ומעובד המידע של רכבת ישראל יהיו מוגנים מפני נזקים סביבתיים (הצפה, שריפה וכדומה).

5.4 הספק יתחייב לניהול רשימת נותני שירותים עדכנית, של בעלי גישה למידע, או לתחנות העבודה ברכבת ישראל, לרבות תפקידיהם וסמכויות הגישה למידע, כפי שהוגדרו ע"י וכן דווח על כל שינוי לרכבת. רשימת נותני השירותים תאושר ע"י הרכבת טרם העסקת העובדים במתן השירותים, נשוא ההתקשרות.

5.5 היה ורלוונטי, הספק יתכנן ויממש מענה ביטחון ואבטחה לכלל הפרויקט, החל משלב קבלת צו התחלת עבודה הראשון בפרויקט ועד סיום העבודות ומסירת המערכת לרכבת ישראל וכן בתקופת התחזוקה.

5.6 המענה יהיה בהתאמה לדרישות האבטחה והביטחון של רכבת ישראל, יעמוד בתקנים המחייבים ובתקנות הרלוונטיות של מדינת ישראל, משטרת ישראל, משרד התחבורה, משרד התשתיות והמשרד לביטחון פנים.

5.7 המענה יתוכנן לכלל הפרויקט וימומש בהתאם לתכנית המימוש ושלבי הפרויקט שהוגדרו במסמך זה ויוגדרו בהתאם להתפתחות הפרויקט על ידי רכבת ישראל.

5.8 התכנית תותאם למענה הביטחון והאבטחה הקיים כיום ברכבת ישראל ותאושר על ידי אגף ביטחון וחרום ברכבת ישראל, טרם יישומה.

5.9 הספק יציג פתרון למניעת גישה למרכיבי מערכת בתחזוקת הציוד, להגנתו ולבקרתו.

5.10 בנוסף לאמור במסמך זה, הספק יטמיע בתכנית הביטחון והאבטחה את כלל ההערות והדרישות הרלוונטיות לפרויקט שיוצגו לו למימוש על ידי גורמי הביטחון של רכבת ישראל.

5.11 תכנית הביטחון והאבטחה תכלול התייחסות בנושאים הבאים:

5.11.1 תיאור תפיסת העל לביטחון ולאבטחה;

5.11.2 ניתוח מצב קיים ואופן השתלבות המענה המוצע למצב הקיים;

5.11.3 מיפוי וניתוח הפערים במצב הקיים והנדרשים להשלמה בעקבות ההערכות למימוש הפרויקט.

5.12 תכולת תכנית ביטחון ואבטחה לפרויקט:

5.12.1 כתיבה והגשת "תכנית על" (ע"ג מסמך הכולל תפיסה, שיטה, משימות והנחיות, הישגים נדרשים, לוחות זמנים, מרשמים, תכניות, תצלומים, מפות וחומר עזר רלוונטי, נהלים, סדרי פעולות וכו').

5.12.2 כתיבה והגשת "תיקי שטח" לכלל מרכיבי הפרויקט, כגון:

5.12.3 מתקני ליבה ומרכזי מערכת.

5.12.4 חדרי תקשורת ומחשבים.

5.12.5 מתקני תשתית (חדרי מתח, מתקני גישה לתשתיות תקשורת וכו').

5.13 מרכיב מימוש התכנית בתחום הבינוי, התשתיות, המערכות והאמצעים המרכיבים את מרכיבי האבטחה והביטחון, לרבות:

5.13.1 גדרות קבועות וזמניות;

5.13.2 מחסומים ושערים קבועים וזמניים;

5.13.3 מערכות אזעקה;

5.13.4 מערכות בקרת כניסה.

5.13.5 חיישנים למיניהם כחלק ממערכת בקרת מערכות המבנה (גלאי נפח/תנועה, הצפה, אש, עשן, פתיחת דלת, פתיחת חלון, הפסקת חשמל)

5.13.6 חדרי תקשורת, ארונות תקשורת, מוקדי תקשורת מקומיים הנדרשים להקמה, כחלק ממענה נדרש למימוש תכנית הביטחון והאבטחה.

5.13.7 סך הדרישות המופיעות בסעיף 5 -5 "ביטחון ואבטחה" לעיל, מהוות את המינימום למימוש ועל הספק להציג תוספות הנדרשות על פי ניסיונו, על מנת לשפר את ההגנה הפיסית מעבר לדרישות המפורטות במסמך זה.

## 6. אירועים חריגים

6.1 הספק ינהל דו"חות איתור ומעקב אירועים חריגים, דיווח וטיפול בהם.

6.2 הספק, או נאמן ההגנה בסייבר מטעמו (ראה סעיף 3.2.5 לעיל), ידווח על כל ליקוי אבטחת-מידע, שיגלה במערכות הספק, תוך לא יותר מ48 שעות מרגע גילוי האירוע.

6.3 ליקויים מהותיים הנוגעים בין במישרין ובין בעקיפין למערכות רכבת ישראל ו/או למערכות- נשוא ההתקשרות, **ידווחו במיידית למרכז הניטור הקיברנטי ברכבת ישראל בטלפון: 08-6533065**

6.4 מחויבות הספק לשיתוף פעולה באירועי סייבר:

6.4.1 בכל אירוע בו מעורב אחד מעובדי הספק, או ממשקיו העסקיים, או שקיים חשד למעורבות שיש עמה השלכה ישירה, או עקיפה על רמת ההגנה בסייבר ברכבת ישראל, או בטחון האינטרסים של רכבת ישראל.

6.4.2 בכל הפרה, או חשד להפרה של חוקים, הנחיות גורמי ההנחיה, תקנות, או נהלי הגנת הסייבר.

6.4.3 בחקירת אירועים, או חשדות, לחריגות אבטחה.

## 7. קניין/זכויות בחומר

7.1 מוצהר בזאת כי לספק אין ולא תהיינה כל זכויות בחומר שיועבר לידיו על ידי רכבת ישראל לצורך ביצוע השירותים לפי הסכם זה והספק יהיה רשאי לעשות שימוש בחומר כאמור, אך ורק במסגרת ולשם ביצוע השירותים ובהתאם לכל יתר הוראות הסכם זה.

7.2 מוצהר בזאת כי רכבת ישראל תהיה בעליו היחידים של כל הזכויות בכל חומר שיתקבל, ייאסף, יוכן ויעובד על ידי הספק במסגרת מתן השירותים לפי הסכם זה, לרבות הדיווחים שהספק מעביר לרכבת ישראל. רכבת ישראל תהיה רשאית לעשות בחומרים כאמור כל שימוש שתמצא לנכון, בכפוף להוראות כל דין.

7.3 הספק יצהיר כי הוא מוותר על זכותו לתבוע כל זכות קניינית מרכבת ישראל ובכלל זה את הזכות לקניין רוחני.

## 8. אי עמידה בדרישות נספח זה

8.1 אי עמידה בדרישות נספח זה, כמוה כהפרה יסודית של הסכם ההתקשרות בין הספק לרכבת, ולרכבת כל התרופות הקנויות לה על פי דין ועל פי מסמכי ההתקשרות. בעת הפרת סעיפי ההתקשרות בנספח זה, תהיה רכבת ישראל רשאית:

8.2 להפסיק באורח חלקי, או מלא את הפעלת המערכת, או השירותים, נשוא ההתקשרות, משיקוליה היא ולדרוש מהספק שיפוי מלא על הנזקים שיגרמו כתוצאה מפעולה זו.

8.3 בכל מקרה יתבע הספק לתקן את הליקויים באורח מיידי ועל חשבונו, לאור הפרת ההסכם.

8.4 בנוסף על הרשום לעיל תהיה נתונה בידי רכבת ישראל הזכות לדרוש מהספק לשאת בעלות סקרי הסיכונים, שיבוצעו ע"י רכבת ישראל, בגין אי עמידת הספק במחויבויותיו, כנדרש לעיל.

## 9. סיום התקשרות

9.1 עם סיום ההתקשרות עם הספק, על הספק לבצע את הפעולות הבאות:

9.2 להחזיר לרכבת ישראל, או לכל גורם מטעמה את כל הרשומות, המדיה, האמצעים, הציוד והרכיבים השייכים לרכבת ישראל- בהם עשה שימוש לצורך עבודתו.

9.3 הספק מתחייב להשמיד כל מידע השייך לרכבת ישראל המצוי ברשותו ואשר לא יימסר לרכבת והכל בכפוף לקיומן של הוראות והנחיות רגולטוריות החלות על הספק.

9.4 הספק יתחייב כי לא נשארו ברשותו כל מסמכים, מידע, או פריטים הנוגעים למערכות הקריטיות.

9.5 הספק יוודא כי הדיסקים הקשיחים אשר הכילו מידע של רכבת ישראל נמחקים בהתאם להוראות תקן FIPS SP 800-88 - Guidelines for Media Sanitation, כאשר יש להתייחס לכל פריט מידע כ"מידע רגיש".

9.6 היה והספק נדרש להמשיך ולהחזיק פריטים כנ"ל, יידרש לחתום על הצהרה בה הוא מתחייב להעביר כל מידע ורכיב הנוגע למערכות קריטיות, רק לגורם מורשה מטעם רכבת ישראל ולאחר קבלת אישור כתוב ממנהל אגף הסייבר ברכבת ישראל (ממונה תמ"ק-רכבת ישראל).