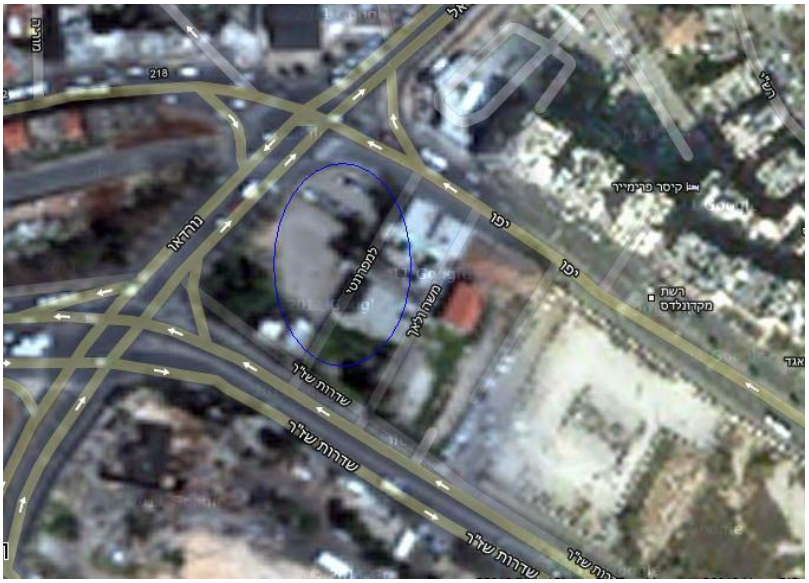
משרד האוצר
מערך סייבר חירום וביטחון
סביבת הביטחון שלך

מערך סייבר חירום וביטחון

פרוגרמת ביטחון

קריית הממשלה המחוזית- נצרת עילית



מסמך זה הינו מסמך רגיש אין לצלם, להעתיק או למסור בכתב או בע״פ כל מידע מתוך מסמך זה, מסמך זה הינו רכושה הבלעדי של מדינת ישראל משרד האוצר מערך סייבר חירום וביטחון , קבלת החוברת אינה מקנה שום זכות במסמך זה ועל המשתתפים בהליך המכרז להשיב את החוברת מיד בתום התהליך עם הגשת ההצעות במסגרת המכרז וזאת ללא השארת עותק או צילום מתוך החוברת בידי המשתתף, הזוכה במכרז יקבל העתק של העותק החתום לאחר הזכייה במכרז

אי מילוי התחייבות זו מהווה עבירה לפי פרק ז׳, ביטחון המדינה יחסי חוץ וסודות רשמיים, לחוק העונשין תשל״ז – 1977.

1 תוכן עניינים

1.1 **הגדרות**

1.1.1 **פירוט:**

1.1.1.1 מידע כללי על המתקן..... 3

1.1.1.2 דרישות מקדימות :חברת מתח נמוך ויועצים 4-9

1.1.1.3 תפיסת הביטחון..... 10

1.1.1.4 מיגון פיזי- דגשים מיוחדים..... 11-27

1.1.1.5 תפיסת ההגנה בסייבר 28-44

1.1.1.6 מתח נמוך- דגשים מיוחדים ואפיון טכני..... 45-68

1.1.1.7 שלבי ההכנות לעבודה..... 69-76

1.1.1.8 ההגנה בסייבר ורציפות תפקודית..... 77-83

1.1.1.9 אחריות 84

1.1.1.10 תיעוד ופעולות נוספות במסגרת תקופת השירות.....85

1.1.1.11 נוסח (דוגמא) לחוזה שירות 86-96

2 מידע כללי על המתקן

2.1 קריית הממשלה המחוזית- נצרת

2.1.1 פירוט:

2.1.1.1 כללי : קרית הממשלה המחוזית בנצרת ממוקמת בסמוך לדרך הציונות ממערב לציר ובסמוך למבנה בית המשפט המחוזי.

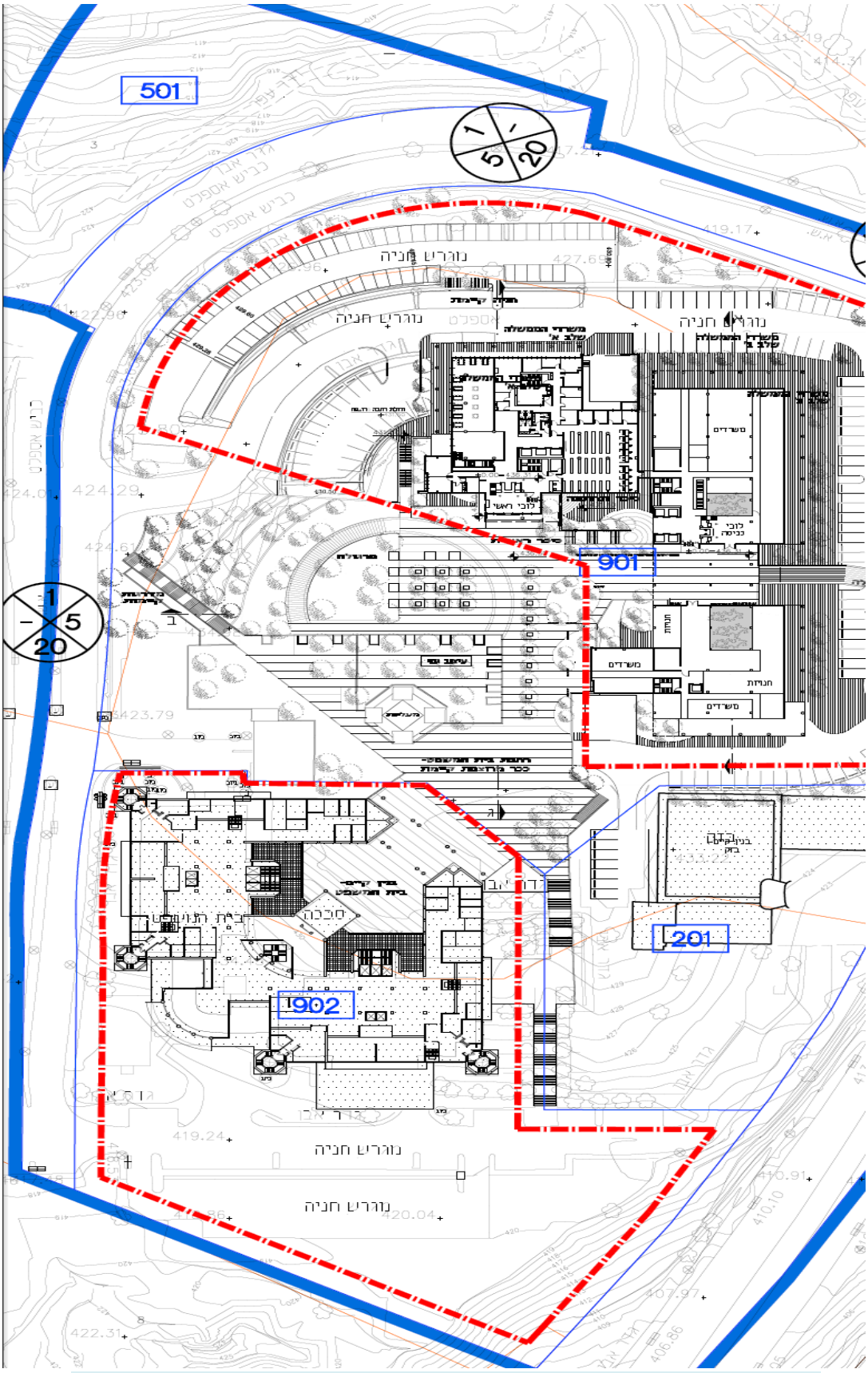
2.1.1.2 קריית הממשלה המחוזית בנצרת בהיותה מיועדת לאכלוס משרדי ממשלה תתוכנן בהתאם להנחיות מיגון ואבטחת מתקנים ממשלתיים- קריות לאום עפ"י הנחיות הגופים המנחים בהתאם לרמת האיום המוגדרת על ידם ועפ"י הנחיות סגן ר' מערך סייבר חירום וביטחון במשרד האוצר

2.1.1.3 לאור מבנה השטח והקירבה הפיזית למבנה בית המשפט תבחן האפשרות ליצירת טריטוריה ביטחונית אחודה לכלל המתחם כחלופה לבידוק ביטחוני נפרד לכל מבנה, במידה ויוחלט על ביצוע טריטוריה אחודה כאמור תוצג התפיסה על כל המשמעויות שלה לזוכה אשר יציג את המשמעות הביצועית והכספית למהלך זה, המזמין רשאי לבצע את העבודה באמצעות הזוכה במכרז זה או בכל דרך אחרת שייבחר ואינו מתחייב לזוכה לבצע את העבודה במסגרת החוזה .

2.1.1.4 מסמך זה מסכם את העקרונות לתכנון מערכות ביטחון במתקן וכולל את המערכות הבאות :

- 2.1.1.4.1 מערכות אבטחה פיזית של המתקן.
- 2.1.1.4.2 מערכות אבטחה לתשתיות מחשוב ותקשורת .
- 2.1.1.4.3 מערכות בקרה ואבטחה אלקטרוניות.
- 2.1.1.4.4 דרישות מיגון ובינוי.
- 2.1.1.4.5 דרישות לאבטחת חניון.
- 2.1.1.4.6 מיגון היקף המבנה.
- 2.1.1.4.7 כלים לתפעול מערך האבטחה.
- 2.1.1.4.8 הגנה בפני התקפות סייבר.

2.1.1.5 הערה : סגן ר' מערך סייבר חירום וביטחון במשרד האוצר הינו נציג הדיור הממשלתי בכל הקשור לאבטחה בפרוייקט זה.


501
901
201
902
נוגרים חניה

3 דרישות מקדימות- חברת המתח הנמוך והיועץ למיגון פיזי

3.1 דרישות מחברת מתח נמוך- קבלן אינטגרצית מערכות הביטחון

3.1.1 פירוט:

3.1.1.1 החברה תעמוד בתו תקן ISO 9001 .

3.1.1.2 החברה תעמיד לידי המזמין אישור ספק מוכר של משרד הביטחון לעבודות מסוג מערכות התראה ומתח נמוך בהיקף בלתי מוגבל.

3.1.1.3 החברה תציג למזמין יכולת מוכחת בהתקנה והפעלה של 5 מערכות ביטחון בסדר גודל דומה ב- שלוש שנים האחרונות כולל רשימת המלצות, הכוללים אינטגרציה ממוחשבת של מערכות בקרת כניסה, איסוף התראות וCCTV וחיבורם באמצעות מערכת שו״ב כולל רשימת ממליצים.

3.1.1.4 היקף כל פרוייקט שתציג החברה יעמוד על מינימום 3 מיליון ₪.

3.1.1.5 החברה לא תורשה להציע מוצר, אביזר, מערכת ותוכנה שהיא הנציגה הבלעדית שלה בארץ אלה תציע מוצר, אביזר, מערכת, תוכנה שקיימות בארץ לפחות שתי חברות הרשאיות למכור אותו. סעיף זה לא יחול על מערכת השו״ב ומערכת בקרת הכניסה .חריגים יאושרו על ידי ס׳ראש מערך סייבר חירום וביטחון בלבד.

3.1.1.6 ספקי / יצרני המוצרים שיוצעו על ידי החברה יהיו בקשרי אספקה בשוק עם לפחות עוד 2 חברות אינטגרציה והתקנה בעלות ניסיון מוכח והמורשות למכור, להתקין ולתת שירות בישראל.

3.1.1.7 החברה תציג בידי המזמין אסמכתא כתובה מיצרני המוצרים והתוכנות אותן עתיד להציע ולספק למציע המאשרת את הכשרת החברה ועובדיה לביצוע התקנות תחזוקה, תמיכה ושדרוג למוצרים והמערכות המוצעות על ידה.

3.1.1.8 לחברה מערך שירות כולל אמצעי תקשורת ומתן שירות 24 שעות ביממה (לא ע״י קבלן משנה) כולל מעבדות שירות ויכולת מוכחת ופועלת לתמיכה ומתן שירות באמצעות צוות מקצועי ויכולת מתן שרות ברמה מבצעית ולא באמצעות מודם מרחוק.

3.1.1.9 התחייבות לביצוע תחזוקה שוטפת ושדרוג המערכות והתוכנות למשך 10 שנים מגמר שנת האחריות בהתאם לנספח שירות שיוגדר על ידי ס.ראש מערך סייבר חירום וביטחון באוצר ובהתאם לחוזה התחזוקה המופיע במסמכי התחזוקה הכללית של מסמכי המכרז .

3.1.1.10 יכולת הנדסית מוכחת לפיתוח ושדרוג מערכות בקרה ממוחשבות ומעסיק לפחות 2 מהנדסי אלקט' ומתכנת.

3.1.1.11 היזם מחויב להביא לאישור של סגן ר' מערך סייבר חירום וביטחון במשרד האוצר את הקבלן המוצע לביצוע העבודות הנ"ל.

3.1.1.12 החברה שתזכה במכרז להתקנת מערכות מנ"מ תהיה מחוייבת לספק את המוצרים והמערכות במחיר זהה למחיר הזכייה שלה במכרז ההקמה לכל אורך תקופת ההתקשרות והסכם השירות בינה לבין היזם ו/או חברת הניהול של משרדי הממשלה הנמצאים במתקן.

3.1.1.13 יובהר כי במידה וקיים מכרז מרכזי בתוקף של מנהל הרכש הממשלתי לעניין רכישה והתקנה ו/או שירות של מערכות מתח נמוך מחוייב היזם לרכוש את המוצרים במסגרת מכרז זה .

3.2 דרישות מיועץ מיגון פיזי:

3.2.1.1 ליועץ אישור מהגופים המנחים הרלוונטיים להיות יועץ מיגון ומופיע ברשימות שלהם המתעדכנות מעת לעת.

3.2.1.2 המשרד יעסיק לפחות 4 עובדים כולל שרטטים, מנהל המשרד הינו מהנדס מוסמך או קונסטרוקטור המעסיק לפחות 2 הנדסאים במשרד בעל נסיון של לפחות 10 שנים בייעוץ בתחום המיגון והמיקלוט לגורמי ביטחון בארץ ובחו"ל, העובדים יעברו הליך סינון ביטחון בהתאם לרמה שייקבע ס' ראש מערך סייבר חירום וביטחון.

3.2.1.3 המשרד נדרש לספק רשימת 3 מתקנים בעלי אופי זהה או דומה שביצע בארץ (יתכן ויתבקש לערוך סיורים והסברים במקומות הנ"ל).
המתקנים חייבים לכלול הן מערכות אבטחה/מיגון בסדר גודל דומה .

3.2.1.4 הייעוץ ותכנון אמצעי המיגון יבוצע ע"י יועצי מיגון ואבטחה מטעם המציע שאושרו ע"י סגן ר' מערך סייבר חירום וביטחון במשרד האוצר ו/או הגורם האחראי מטעם הדיור הממשלתי. על המתכנן להיות בעל ניסיון בנושאי מיגון פיזי בכלל ותכנון מיגון פיזי בקריות לאום או מתקנים ביטחוניים מוגנים יהוו יתרון.

3.2.1.5 הצעת תכנון המיגון הפיזי הכוללת וכל פרטיה תוצג לסגן ר' מערך סייבר חירום וביטחון במשרד האוצר ונציג המזמין לאישור התפיסה הכללית והאמצעים השונים לפני כניסה לתכנון מפורט. כמו כן , כל שלב בתכנון המפורט יאושרו בכתב.

3.2.1.6 מערכות המיגון הפיסי בבניין כוללות מספר אלמנטים אשר אמורים לעמוד באחד או מספר מהאיומים הרשומים ברשימת האיומים המאושרת מראש:

3.2.1.6.1 ירי .

3.2.1.6.2 התמוטטות שרשרת כתוצאה מפיצוץ/רעידת אדמה.

3.2.1.6.3 הדף כתוצאה מרכב תופת או מטען נישא או נייח.

3.2.1.6.4 פריצה של רכב למטרת ניגוח או התקרבות.

3.2.1.6.5 פריצה אלימה של אדם בודד או המון.

3.2.1.6.6 פריצה שקטה / סמויה.

3.2.1.6.7 הפרעות סדר ציבורי / וונדליזם.

3.2.1.7 בכל אתר ומבנה , יש לקבל מסגן ר' מערך סייבר חירום וביטחון במשרד האוצר התייחסות ספציפית לאיומים הנ"ל בהתאם למיקום המבנה ואופיו.

3.2.1.8 מערכות המיגון הפיסי יכללו לפחות את הנושאים הבאים :

3.2.1.8.1 כספת להפקדת נשק מבקרים.

3.2.1.8.2 כספת נשק מרכזית עפ"י תקן משטרה.

3.2.1.8.3 מניעת התמוטטות שרשרת.

3.2.1.8.4 חלונות מוגני הדף .

3.2.1.8.5 חלונות מוגני פריצה.

3.2.1.8.6 דלתות מוגני פריצה (במעטפת חיצונית, בדלתות הכניסה הראשיות ליחידות בחדרי תקשורת מחשבים חשמל וכו', ביחידות מסווגת).

3.2.1.8.7 עמדות חיצוניות לשומרים מוגנות דריסה/ירי ומזג אוויר - שמש וגשם .

3.2.1.8.8 חסימות סטטיות ושערים נגד רכב מתפרץ .

3.2.1.8.9 חדרים מוגני פריצה שקטה ואלימה (תקשורת, ביטחון, ארכיבים, כספות, חדרים ברמת סודי).

3.2.1.8.10 אזורים מוגני הדף (אזורים "הכי מוגנים שיש" לפעילות בשעת חירום).

3.2.1.8.11 אזורים מוגנים לפעילות המשרד במצב חירום לאומי (מיגון ברמת ממ"ד / ממ"ק/ חל"כ).

3.2.1.8.12 אזורים מוגנים פיזית עבור אח"מ (לשכות מנהלים, עובדים מאויימים).

3.2.1.8.13 חדר בקרה בטחוני מוגן קונבציונאלי ובלתי קונבנציונאלי לפעילות במצב חירום לאומי בהתאם לאיום הייחוס הספציפי למתקן.

3.2.1.9 יובהר כי מיגון המתקן יהיה בהתאם לאמור במסמך זה ובהתאם לאיום היחוס המעודכן בעת תחילת העבודות .

הערה : המזמין עפ"י שיקול דעתו יעמיד יועץ צל לפרוייקט .

3.3 דרישות מחברת יעוץ/תכנון טכנולוגי למערכות אבטחה.

3.3.1 תנאי סף מקצועיים :

3.3.1.1 למציע ותק של 10 שנים לפחות במתן שרותי יעוץ, אפיון, תיכנון ופיקוח על מערכות ביטחון, בקרה ותקשורת.

3.3.1.2 המציע ביצע ב- 10 השנים האחרונות תכנון ופיקוח של לפחות ארבעה בעלי אופי דומה אשר בוצעו בארץ הכוללים – מערכות אלקטרוניות מוכללות(אינטגרטיביות) בהיקף כספי של שלושה מליון ₪ לכול פרויקט.

3.3.1.3 המציע הינו בעל משרד פעיל ב- 10 שנים האחרונות לפחות ומעסיק לפחות- 4 עובדים מקצועיים ובכללם :

3.3.1.3.1 מהנדס אלקטרוניקה או מחשבים ואו בוגר תואר ראשון במדעי המחשב.

3.3.1.3.2 הנדסאי/ טכנאי אלקטרוניקה או מחשבים.

3.3.1.3.3 שרטט אוטוקד.

3.3.1.3.4 מנהל פרויקטים/ משרד בעל נסיון של לפחות – 10 שנים.

3.3.1.4 המציע הינו בעל הסמכה תקפה ממוסד מוכר לתקן איזו 9000 .

3.3.1.5 המציע הינו ספק מוכר מוכר בתוקף של משרד הביטחון.

3.3.1.6 על העובדים במשרד העוסקים בפרויקט לעבור הליך סינון ביטחון בהתאם לרמה שיקבע ס. ראש מערך סייבר חירום וביטחון במשרד האוצר.

3.3.1.7 הייעוץ והתכנון של אמצעי הביטחון הטכנולוגיים יבוצעו ע"י יועץ מטעם המציע ויאושרו ע"י סגן ר' מערך סייבר חירום וביטחון במשרד האוצר ו/או הגורם האחראי מטעם הדיור הממשלתי. על היועץ להיות בעל ניסיון בנושאי אבטחה ומערכות מנ"מ אינטגרציה תקשורת ובתכנון מערכות אבטחה טכנולוגיות לפרוייקטים ביטחוניים גדולים באותו סדר גודל במהלך העשור האחרון בלפחות חמשה מתקנים.

3.3.2 הליך אישור תכנון המערכות :

3.3.2.1 הצעת תכנון המערכות והאבטחה הכוללת וכל פרטיה תוצג לסגן ר' מערך סייבר חירום וביטחון במשרד האוצר ונציג המזמין לאישור התפיסה הכללית והאמצעים השונים לפני כניסה לתכנון מפורט. כמו

כן , כל שלב בתכנון המפורט יאושר בכתב.

3.3.2.2 מערכות המנ"מ בבניין כוללות מספר אלמנטים אשר אמורים לעמוד באחד או מספר מהאיומים הרשומים ברשימת האיומים המאושרת מראש :

3.3.2.2.1 החדרת אמצעים בהתאם לאיום הייחוס של הגופים המנחים .

3.3.2.2.2 התפרצות רכבים והתקרבות למבנה.

3.3.2.2.3 חדירה אלימה/ בכיסוי.

3.3.2.2.4 איתור חריגים וחשודים.

3.3.2.2.5 פריצה אלימה של אדם בודד או המון.

3.3.2.2.6 איתור חריגים בתנועה מחוץ ובתוך שטחי המתקן

3.3.2.2.7 פריצה שקטה / סמויה ביום ובלילה.

3.3.2.2.8 הפרעות סדר ציבורי / וונדליזם.

3.3.3 בכל אתר ומבנה , יש לקבל מסגן ר' מערך סייבר חירום וביטחון במשרד האוצר התייחסות ספציפית לאיומים הנ"ל בהתאם למיקום המבנה ואופיו.

3.3.3.1 מערכות המנ"מ יכללו לפחות את הנושאים הבאים :

3.3.3.1.1 מערכת שו"ב מרכזית (חיבור למרכז בקרה ארצי שו"ב על).

3.3.3.1.2 מערכת בקרת פריצה ממוחשבת.

3.3.3.1.3 מערכת בקרת כניסה מבוססת כרטיסי תמו"ז וביומטריה.

3.3.3.1.4 מערכת טמ"ס – IP דיגיטלית מערכת הקלטה ותוכנת אנליטיקה.

3.3.3.1.5 מערכות בקרה ממוחשבות ברשת ביטחון ייעודית .

3.3.3.1.6 עמדות בקרת כניסה ראשיות בכניסה למתחם ועמדות משניות .

3.3.3.1.7 עמדות בקרה משניות (חניונים, כניסת ספקים וכו') .

3.3.3.1.8 חסימות סטטיות ושערים נגד רכב מתפרץ .

3.3.3.1.9 חדרים מוגני פריצה שקטה ואלימה (תקשורת, ביטחון, ארכיבים,כספות, חדרים ברמת סודי).

3.3.3.1.10 אזורים מוגנים לפעילות המשרד במצב חירום לאומי (מיגון ברמת ממ"ד / ממ"ק/ חל"כ).

3.3.3.1.11 אזורים מוגנים פיזית עבור אח"מ (לשכות שרים, עובדים מאויימים).

3.3.3.1.12 חדר בקרה בטחוני מוגן קונבציונאלי ובלתי קונבנציונאלי

לפעילות במצב חירום לאומי.

3.3.3.1.13 אמצעי איתור ואיסוף נתונים להגנה מפני תקיפות סייבר וחיבור לרכיבי המערכת.

3.3.4 היזם יעמיד יועץ נוסף בתחום ההגנה בסייבר ורציפות תפקודית בעל נסיון בתחומים אלו במערכות הביטחון השונות (צה"ל שב"כ משרד ביטחון וממשלה) אשר עסק בתחום ייעוץ זה לפחות בשנתיים האחרונות וביצע פרוייקטים בתחום ההגנה בסייבר עבור גופים אלו, היועץ יאושר על ידי מערך סייבר חירום וביטחון(ראה המפורט בפרק- 9 במסמך זה) .

3.3.5 **יובהר כי מיגון המתקן יהיה בהתאם לאמור במסמך זה ובהתאם לאיום היחוס המעודכן בעת תחילת העבודות והמותאם למתקן באופן ספציפי .**

הערה : המזמין עפ"י שיקול דעתו יעמיד יועץ צל לפרוייקט .

3.4 דרישות כלליות מחברת המתח הנמוך –אינטגרטור מערכות הביטחון והיזם המיגון הפיזי:

3.4.1 פירוט:

3.4.1.1 לספק ולהתקין את כל האמצעים הטכנולוגיים כולל גם החווט והתשתיות הרלוונטיות על פי המפרטים הטכניים התוכניות וכתבי הכמויות כפי שאושרו ע"י המזמינה.

3.4.1.2 לקיים ולהיות שותף בהדרכות למפעילים בהתאם לדרישת הלקוח וסגן ר' מערך סייבר חירום וביטחון במשרד האוצר .

3.4.1.3 החברה והקבלן ידרשו לספק תיעוד מלא של כל המערכות הפיזיות והטכנולוגיות כולל שרטוטי " as made " בהתאם לדרישות התכנון והמפרט הטכני.

3.4.1.4 הקבלן / החברה המבצעת ידרשו להגיש הצעה למתן שרות ותחזוקה ולספק שירותי תחזוקה לאחר תקופה של שנתיים אחריות ללא תשלום , לפחות לתקופה של 10 שנים נוספות בהתאם למחיר שיקבע במסגרת מכרז שבו זכתה חברת האינטגרציה.

3.4.1.5 תנאי הסף כאן מתייחסים לקבלן המתעתד לבצע את מערכות המתח נמוך והטכנולוגיות בבניין כמפורט לעיל בסעיף 3.3.3.

3.4.1.6 אישור ביצוע ניסוי או חישוב המוכיח את ביצועי המוצר המסופק. על הקבלן / חברה המבצעת להוכיח ביצוע פרויקטים עם אמצעים דומים עבור גורם ממשלתי בעל צרכים והיקף עבודה דומים.

3.4.1.7 אסמכתאות כתובות מיצרני המוצרים אותן מציע לספק המאשרות את

הכשרת החברה ועובדיה לביצוע התקנות, תחזוקה, למוצרים המוצעים על ידו.

3.4.1.8 על הקבלן / החברה לאשר שצורת ההתקנה בבניין אכן עומדת בקנה אחד עם הנדרש לצורך רמת הביצועים הנדרשת

3.4.1.9 בחירת קבלן מערכות המנ"מ והביטחון ואישורו כקבלן מבצע בפרויקט כפופה לאישור סגן ר' מערך סייבר חירום וביטחון במשרד האוצר והדיור הממשלתי.

3.4.1.10 הקבלן ועובדיו יידרשו לעמוד ברמת סיווג בטחוני שיקבע ע"י סגן ר' מערך סייבר חירום וביטחון במשרד האוצר.

4 תפיסת הביטחון

4.1 פירוט תפיסת הביטחון

4.1.1 פירוט:

4.1.1.1 תכנית האבטחה מחולקת מתודית לשלושה מעגלים גיאוגרפיים :

4.1.1.1.1 <u>מעגל אבטחה היקפי (חיצוני)</u> : הכולל את גבולות המגרש, גבולות המבנה והשטחים שביניהם, הרחובות הציבוריים, הכניסות אל המגרש, הגידור, הכבישים שבהיקף המגרש והשטחים והמבנים השולטים והמשפיעים על אבטחת המתחם והמבנה.

4.1.1.1.2 <u>מעטפת הבניין (ביניים)</u> : הכולל את קירות המבנה ההיקפיים- כולל גג, חניונים פנימיים, כל הפתחים במעטפת הבניין- שערים, דלתות וחלונות, לובי הכניסה הראשי , הכניסה לחניונים וכל השטחים הפנימיים והמשותפים.

4.1.1.1.3 <u>המבנה (פנימי)</u> : הכולל את קומת הכניסה / קרקע, קומת מרתפים, קבלת קהל, קומות משרדים, אזורים ממודרים בקומות ממודרות, אזורים ממודרים כולל לשכות שרים ומנכ"לים, חדרי מדרגות ופירים חוצי קומות, מעליות, חדרי תשתיות חיוניות חשמל,תקשורת וכו'), מערכות ממודרות חוצי קומות, תקשורת, מחשב, אוורור, אזורים מוגני אב"כ, הדף ורסס כולל מרחבים מוגנים.

4.1.1.2 על מכלול המעגלים תשלוט מערכת שליטה ובקרה (מבוססת שו"ב) שתמוקם בחדר בקרה משולב לביטחון ובקרת המבנה, שליטה/בקרה

על כל מעגלי האבטחה כמפורט לעיל החל ממעגל האבטחה ההיקפי דרך מעגל הביניים וכלה במעגל הפנימי.

4.1.1.3 מערכות הביטחון יחוברו ל"שו"ב על" שמוקם במוקד הבקרה הארצי בבניין ג'נרי 2 או בכל מקום אחר שיוגדר על ידי ס' ראש מערך סייבר חירום וביטחון . חיבור זה יאפשר קבלת התראות ביטחון וצפייה במוקד המקומי פירוט יתר בנושא זה יועבר לקבלן לאחר גיבוש התפיסה המבצעית הטכנית.

הערה : מערכות האבטחה מתפתחות באופן קבוע, וצפוי כי במהלך השנים מכתיבת פרוגרמה זו ועד להקמת המערכות במבנה תהיה התפתחות טכנולוגית וייתכן כי יהיו מערכות / טכנולוגיות חדשות אשר יהיה צורך בשילובן כחלק בלתי נפרד מהמתקן החדש, היזם מתחייב לאפשר החלפת מערכות המוגדרות במסמך זה במערכות/טכנולוגיות חדשות אלו בהתאם להחלטת ס. ראש מערך סייבר חירום וביטחון במשרד האוצר וזאת במסגרת אומדן העלויות לפרוייקט, על אף שלא הוגדרו המערכות הללו במסמך זה.

5 דגשים מיוחדים התואמים את תפיסת הביטחון - מיגון פיזי

5.1 כללי

5.1.1 כללי:

5.1.1.1 הבניין ימוגן כנגד איומי הייחוס המופצים מעת לעת ע"י הגופים המנחים (מ"י, שב"כ, רח"ל ופיקוד העורף) אשר יופצו ע"י סגן ר' מערך סייבר חירום וביטחון במשרד האוצר וייחיבו את היזם בתכנון ע"י יועץ מיגון פיזי המאושר לייעץ לפרוייקטים מטעם הגופים המנחים, יודגש כי המזמין רשאי להגדיר איום ייחוס אחר מהמוגדר על ידי הגופים המנחים אשר מחמיר על איום היחוס שלהם וזאת בהתאם לשיקול דעתו הבלעדי.

5.1.1.2 תכנון המיגון הפיזי יתן מענה בכל מעגלי האבטחה למניעת פגיעה במבנה ולצמצום הנפגעים כנגד איומי הייחוס המוגדרים.

5.1.1.3 יועץ המיגון הפיזי יכין תוכנית בה יציג את תפיסת המיגון כמענה לאיומי הייחוס המוגדרים וכן יציג את הפתרונות המוצעים על ידו לצמצום כמות הנפגעים כנגד איום הייחוס בכל מתווה אפשרי כנגד המושא המאובטח בייחס לתכנון האדריכלי המוצג לפרוייקט.

5.1.1.4 תכנון המיגון יועבר לבחינה של סגן ר' מערך סייבר חירום וביטחון במשרד האוצר או מי מטעמו לפני תכנון מפורט וכן לפני ביצוע לאישורו לפני פרסום מכרזי הביצוע רלוונטיים (בטונים,אלומיניום ,

וכו').

5.2 תכנון מבנה וקונסטרוקציה

5.2.1 פירוט:

5.2.1.1 הבניין המיועד יעמוד בדרישות תקני הבניה המחמירים לעמידות ברעידת אדמה והתמודדות עם התמוטטות בשרשרת כתוצאה מפיצוץ עפ"י איום הייחוס.

5.2.1.2 שלד המבנה יתוכנן באופן שאיבוד עמוד או קורה מרכזית כתוצאה מפיצוץ או כל איום אחר לא יגרמו להתמוטטות בשרשרת או לנזק משמעותי.

5.2.1.3 עמודים/קורות קריטיים חשופים לאיום יחוזקו נקודתית לפי הצורך בהתאם למרחקם מנקודת האיום הרלוונטית (למשל קונסטורקציה הקרובה לכביש) .

5.2.1.4 הפרטים למיגון יופיעו בתוכניות בינוי/קונסטרוקציה לביצוע ויאושרו ע"י יועץ המיגון לפני הביצוע בחתימה על תוכניות לביצוע.

5.2.1.5 תוכנית הקונסטרוקציה תצטרך להיבחן על רקע ההמלצות הנ"ל.

יועץ המיגון פיזי יאשר בכתב על גבי התוכניות כי המיגון שבוצע במתקן עומד כנגד איום הייחוס שהוגדר על ידי הגופים המנחים באמצעות ס' ראש מערך סייבר חירום וביטחון במשרד האוצר ומתחייב כי הוא ביצע את כל החישובים הנדרשים לבחינת עמידת המבנה כנגד איום ייחוס זה.

5.3 מעגל חיצוני: נושאי שטח, אדריכלות נוף , חניונים וחצרות:

5.3.1 פירוט:

5.3.1.1 יש לשאוף כי המבנה ימוקם במרכז חצר מוקפת גדר או חומה וכניסות סגורות ע"י שערים או דלתות.

5.3.1.2 גבול המגרש יוגן באמצעות עמודים / שערים או פיתוח סביבה לעצירת רכב/אופנוע מתפרץ/רכב תופת עפ"י תקן כמוגדר במפרט הטכני של מסמך זה.

5.3.1.3 מניעת הגעת רכב שאינו בדוק למרחק שלא ייפחת מ- 10 מטרים מקו המבנה.

5.3.1.4 באין אפשרות להקים גדר של ממש בחלק מגבולות המגרש יש לשלב בהיקף הגדר "מכשול" אדריכלי כלשהו (מדרגות, שינוי מפלס, עמודי

חסימה, אדניות, ריהוט גן וכד׳) .

5.3.1.5 תנועת מבקרים ואזרחים – יש לתכנן נתיב מוגדר וברור להולכי רגל מהמרחב הציבורי לתוך החצר וכן מהחצר הציבורית למרחב הפנימי (לובאי הבידוק) ובכך יאפשרו לתעל את זרם המבקרים לכניסה בה מבוצע הבידוק בצורה המאפשרת שליטה מירבית על הנכנסים, במסגרת שליטה זו יעשה שימוש גם במצלמות טמ״ס השולטים על המתחם.

5.3.1.6 חצר המתקן והגינון יתוכנן באופן שיאפשר סריקה קלה ופשוטה תוך הימנעות ממקומות מסתור של חפצים חשודים וימנע גישה לקרבת קירות המבנה ויכולת התמנה באזורי ריכוז קהל והכניסות .

5.3.1.7 לחצר תתוכנן תאורת לילה שתאפשר זיהוי קל ומהיר בעין ובמצלמת cctv של כל אדם שיסתובב בחצר או בהיקף המבנה.

5.3.1.8 בהיקף החצר ובעיקר באזור הפתחים יתוכננו עמדות אבטחה שתהיינה מוגנות משמש, רוח וגשם וימוקמו בנקודות הגישה הרגליות והרכובות למתחם.

5.3.1.9 הכניסות לחניונים יתוכננו תוך לקיחה בחשבון כי יתכנו עיכובי רכב חשוד לצורך בידוק ו/או סיבוב לאחור לאחר סירוב כניסה ללא כניסה לשטח המתחם המוגן.

5.3.1.10 הכניסות לחניונים פנימיים יתוכננו כשלצידן מבנה שומר מוגן ממפגעי מזג אוויר ועמיד כנגד פריצה אלימה לפחות ל 15 דקות וכן כנגד ירי וכולל חיבור למערכות הביטחון כולל פתיחת השערים החשמליים במקביל לשליטה על השערים ממוקד הבקרה בבניין,מסך לצפייה בטמ״ס רלוונטי וכן אמצעי תקשורת עם חדר הבקרה לביטחון.

5.3.1.11 יש לתכנן מיגון למתחם הפנימי כנגד התפרצות קהל ומפגינים לחצר הציבורית ונעילת לילה , עמידות המיגון תהיה כנגד לחץ קהל של 500 ק״ג למטר לפחות וניתן לבצע נעילה מהירה חשמלית דרך מוקד הבקרה של מחסומי המיגון לכלל המתחם, כמו כן יש לתכנן פרט מעקב טיפוס בקצה הגדר המקיפה את שטח המבנה למניעת טיפוס מפגינים או מניעת חדירה לשטח המתחם.

5.3.1.12 יש לאפשר , במסגרת החצר ההיקפית של המבנה, שטח שיוגדר כשטח היערכות לכוחות חירום והצלה.

5.4 מעגל ביניים: אדריכלות המבנה- מעטפת:

5.4.1 פירוט:

5.4.1.1 יש לשאוף למספר פתחים קטן ככל האפשר במפלס הקרקע כדי להקטין הצורך בהגנה פיזית וטכנולוגית (עלות גבוהה) ומתוך מטרה למנוע חדירה בלתי מורשית לבניין אם ע״י פריצה שקטה או פריצה אלימה עפ״י הנחיות הגופים המנחים והנחיות הדיור הממשלתי,

לעמידות של 5- 15 דקות כנגד פריצה אלימה בהתאם לקביעת ס' ראש מערך סייבר חירום וביטחון באוצר, דבר זה יתבצע ע"י מערכות גילוי פריצה בנוסף להגנה פיזית כדוגמת סורגים או חלונות מוגנים פריצה המאושרים ועומדים בתקן הגופים המנחים לעמידות כנ"ל.

5.4.1.2 קיר המעטפת, במיוחד בקומת הקרקע, יהיה בניה מסיבית (בטון/לבנים מלאות) בכדי להקטין הפגיעות של הקומה כנגד האיומים השונים ולהקטין הצורך במיגון.

5.4.1.3 יש לשאוף לתכנן מבנה עם שטחי חלון היקפיים קטנים ככל האפשר בדגש על הקומות הנמוכות והכל בייחס ישיר למרחק המינימאלי מאיום הייחוס המוגדר למבנה, יועץ המיגון יציג את המענה לאישור לפני תכנון מפורט וכמובן יאשר ביצוע עפ"י הנחיותיו וכי אכן המבנה עומד כנגד איום הייחוס . שטחי חלון גדולים יחייבו מיגונם בעלות גבוהה (ראה פרק מפרט טכני במסמך זה).

5.4.1.4 קירות מסך בהיקף המבנה (במידה ומתוכננים למרות שאינם מומלצים) יהיו בעלי מסגרת מלאה בהיקף הזכוכית בשונה מקיר מסך זכוכית נקייה שמאוד קשה להגנה, פרט סופי לביצוע לאחר אישור יועץ המיגון כי אכן עומד כנגד איום הייחוס.

5.4.1.5 כל החלונות, הדלתות וקירות מסך הזכוכית בבניין- מקומת הקרקע ועד קומה שלישית לפחות בין 7-5 מטרים מעל למקום עמידה יהיו מוגנים כנגד פריצה אלימה למשך 15-5 דקות כמוגדר בפרק המפרט הטכני במסמך.

5.4.1.6 כל החלונות וחזיתות הזכוכית יתוכננו לעמידות מיטבית בהדפי פיצוץ בהתאם להנחיות עבור קריות הממשלה לעמידות כנגד רכב תופת שיתפוצץ בנקודת ההגעה הקרובה ביותר הרלוונטית לרכב לא בדוק כמוגדר בפרק המפרט הטכני במסמך זה.

5.4.1.7 תתוכנן מערכות התרעת חדירה בהיקף המבנה ובפתחים.

5.4.1.8 תתוכנן מערכות תצפית בכל היקף המבנה לכיסוי תצפית של כל הפתחים ואימות אזעקות לכל אחד מהגלאי פריצה. המערכת תתוכנן כך שתתן תמונה טובה ואמינה יכולת ניתוח ושחזור אירועים מלאה ואיכותית ומהירה קרוב לזמן אמת במערכת תשולב אלגוריתמיקה מתקדמת ושיפור קבלת ההתראות והקטנת התראות שוו / מתרידות.

5.4.1.9 יתוכננו פתחי מילוט תקניים ללא הפחתה ברמת העמידות לפריצה אלימה שנקבעה, כולל השהיית פתיחה לפי התקן ואישור רשויות הבטיחות.

5.4.1.10 יש לתכנן מילוט מהחניון אל השטח הציבורי החיצוני ולא לתוך שטח המבנה.

יש לתכנן מעליות חניון ליציאה לשטח הציבורי לפני אזור הבידוק הבטחוני בתוך המבנה כך שכל מי שעולה במעלית/מדרגות החניון יגיע לשטח ציבורי ולא לתוך השטח הסטרילי.

5.4.1.11 התכנון יאפשר סגירת חירום מהירה של המבנה/ החניון כולל פתחי

המילוט במקרה הצורך באמצעות שליטה על כלל הפתחים ממוקד בקרת הביטחון באמצעות מחסומים ושערים חשמליים וממונעים ויכולת נעילה מרחוק .

5.5 מעגל ביניים: לובי כניסה ראשי- עקרונות כניסת קהל ועובדים:

5.5.1 פירוט:

5.5.1.1 כניסת קהל, מבקרים ועובדים מתקיימת בד״כ דרך הכניסה הראשית, בתכנון הלובי הראשי יש לקחת בחשבון את הצורך בבקרה מלאה של כל אחד מהנכנסים, בידוק בטחוני של המבקרים, הצטברות תורים (במקרה של קבלת קהל) ואפשרות אירועים ביטחוניים באזור זה כולל הפרעות סדר ופיגועים.

יש להציג תכנון עם כניסה ראשית אחת לכלל חלקי המבנה.

חלוקה לפי ריכוז המשרדים מקבלי הקהל וריכוז המשרדים שלא

מקבלים קהל.

5.5.1.2 במסגרת תכנון זה יש לקחת בחשבון ציר תנועה נוח לעובדים מורשי כניסה באצעות בקרת כניסה ממוחשבת (קורא קירבה עפ״י המפרט הטכני) המבוססת על כרטיס תמו״ז של עובדי מדינה, תאי סינון הינם אופציה נוספת שניתן לבחון בייחס לתכנון מפורט.

5.5.1.3 תתאפשר יציאת מבקרים ללא הפרעה לתהליך הכניסה וללא מתן אפשרות לכניסה לא מבוקרת מבחוץ דרך פתח זה.

5.5.1.4 יש לשאוף לאפשר מתן שירות רחב ככל האפשר ללא צורך להיכנס לתוך הבניין ולעבור את הבידוק הביטחוני. דבר זה יכול להיעשות ע״י דלפקי שירות אוטומטיים זיהוי ביומטרי וכו׳, מערכת קבלת טפסים וכדומה כפי שנעשה במספר מתקנים משרדים ברחבי הארץ ,יש לשאוף שעמדות אלו ימוקמו מחוץ לשטחים הסטריליים ולפני עמדות הבידוק ניתן לבצע באמצעות אשנבי שירות הפונים לחצרות ולשטחים הציבוריים או באמצעות הצבת מערכות/עמדות ממוחשבות בשטחים הציבוריים.

5.5.1.5 יש לתכנן לובאי כניסה המאפשר בידוק מלא של הנכנסים הן ידני והן באמצעים טכניים שמשתנים לאורך השנים. שטח הרצפה הנדרש יתוכנן עפ״י כמות המבקרים הצפויים ותכנון בזמן הנדרש למעבר הבידוק אך תוך התייחסות למשקל הציוד הביטחוני ושטח הרצפה לה הוא נזקק :

5.5.1.5.1 מינימום שטח רצפה למכונת שיקוף : 100X300 ס״מ.

5.5.1.5.2 מינימום שטח רצפה לשער מגלה מתכות : 130X130 ס״מ.

5.5.1.6 יש לתכנן מרחק של לפחות 50 ס״מ בין שער מגלה המתכות לבין כל אביזר מתכתי אחר ובפרט מעברים מהירים ומכונות שיקוף, במרווחים הללו יתוכננו מעקות על פי הצורך והדרישות.

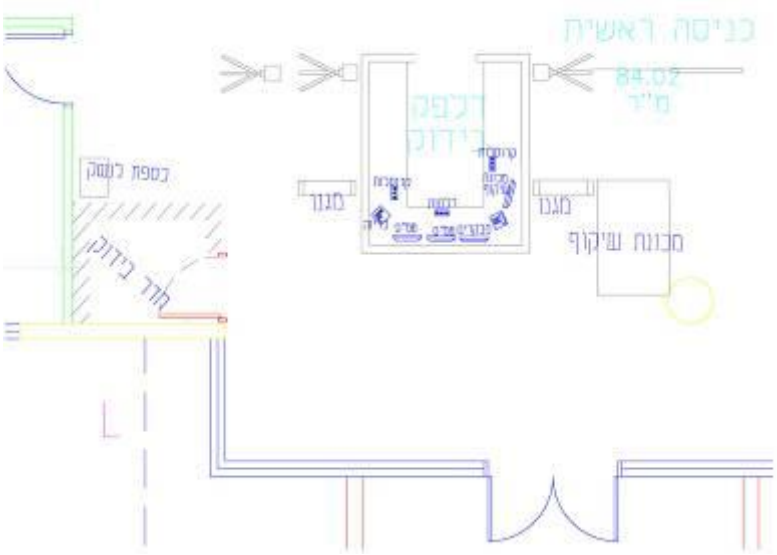
5.5.1.7 הכניסה למבנה תעשה דרך שערים חשמליים מהירים נמוכים מופעלים ע״י בקרת כניסה ומערכת מניעה לכניסה כפולה וממוקמות באופן שלא תאפשר כניסה מבלי לעבור דרכן. בחלק מהמקרים יתוכננו קרוסלות בגובה מלא, קרוסלות זכוכית או שערים נפתחים לפי הצורך והתכנון הספציפי.

5.5.1.8 יותקנו מעקות זכוכית מחוסמת בכל המרווחים הקיימים בתכנון , תכנון מערך הכניסה הסופי יאושר על ידי נציג המזמין.

5.5.1.9 החלטה לגבי כמות נתיבי הכניסה של מבקרים הנדרשת בלובי תעשה כך שלא ייווצר מצב של המתנה בתור של יותר מ-5 דקות, עפ״י ניתוח כמות מבקרים צפוי בזמן שיא (מפתח של 25 שניות לבדיקת אדם בממוצע).

5.5.1.10 בכל מערך כניסה ראשי תתוכנן עמדת ביטחון בכניסה שתפקח על הבידוק ותפעול מערך הכניסה. גודל העמדה, מיקומה והציוד שבה יתוכנן בהתאם לצרכים הספציפיים.

5.5.1.11 ההצבה המועדפת הינה דלפק מרכזי עם שני נתיבי כניסה משני הצדדים (ראה סקיצה) :



5.5.1.12 עמדות אבטחה שולטות -

5.5.1.13 ניתן לתכנן גם עמדות בידוק בודדות עם דלפק ועמדת בידוק בודדת .

5.5.1.14 בהתאם לצפי של כמות ואופי המבקרים, יש לתכנן ניתוב, ושילוט יעיל אשר יקצר את התהליכים למבקרים מוזמנים או מוכרים. כמו כן

כמות עמדות הבידוק ייקבעו בהתאם לצפי כמות המבקרים המקסימלי בשעות קבלת הקהל ויותאמו לכל מבנה בהתאם למשרדים המאכלסים.

5.5.1.15 בלובי הכניסה ולפני מערך הבידוק יתוכנן חדרון קטן לבידוק גופני. החדרון יכלול דלת ננעלת מבפנים ווילון פנימי. שטחו המינימאלי יהיה 1.5X2 מ׳

5.5.1.16 דלתות הכניסה והלובי המתואר לעיל יתוכננו תוך לקיחה בחשבון מבנה יעיל מבחינה אנרגטית של מיזוג האוויר בהנחה שבאזור הסמוך לדלתות ישהו אנשים. לכן יש לתכנן מערך דלתות אשר ישמור על השפעה מינימאלית של הטמפרטורה בחוץ על הלובי, (כדוגמת דלתות מסתובבות).

5.5.1.17 במבנה מקבל קהל רב מומלץ לתכנן אזור המתנה שיאפשר המתנה למבקרים בזמן שהם ממתינים לאישור כניסה. תכנון השטח הנדרש והריהוט, בהתאם לכמות ואופי המבקרים הצפויים, במקרה של קבלת קהל הממתין מחוץ למבנה יש להכיל את הקהל באזור שניתן לאבטח אותו באמצעים ובמיגון וכן מתן מענה לממתינים כנגד מזג אוויר .

5.5.1.18 בכניסה, לפני קו הבידוק, תמוקם כספת / ארוניות לאחסון עצמי של כלי נשק. מפרט לכספת זו בהתאם להנחיות משטרת ישראל שמשתנה מפעם לפעם.

5.5.1.19 נדרש כי נתיבי היציאה מהבניין יהיו בסמוך לאזור כניסת הקהל באופן אשר יאפשר בקרת המאבטחים ויחסוך עלויות ביצוע ותפעול.

5.5.1.20 בלובי הכניסה הראשי יתוכנן שולחן לובי הכולל עמדות עבודה לבודקים. דלפק השולחן יהיה מחומרים עמידים נגד שריטות כדוגמת שיש או זכוכית. עמדת העבודה תכיל את אמצעי האבטחה הנדרשים לשליטה על האמצעים בלובי (סבסבות,דלתות וכדומה) מערכת קליינט למערכת טמ״ס וכן מחשב מנהלתי המחובר למערכת הזמנת מבקרים ואינטרנט קשר עם בקרת הביטחון, נקודת כריזה נוספת ופנל משנה למערכת גילוי אש. כלל האמצעים יושקעו בשולחן הבקרה בתוך פנל אלומיניום בזוית תפעול נוחה ללא הסתרה של הכניסה והלובי כאשר המאבטח יושב.

5.5.1.21 לובי הכניסה הראשית ירושת במצלמות מעגל סגור שיופעלו ממוקד הבקרה אשר יאפשרו שליטה מלאה על הנעשה בתוך לובי קבלת הקהל יותקנו מצלמות אשר יכסו את מסלולי הכניסה והיציאה משני הכיוונים לזיהוי הנכנסים והיוצאים ומצלמות נוספות אשר יכסו את כלל מרחב לובי הכניסה, כמו כן יותקנו מעל עמדות הבידוק הביטחוני מכשירי הקלטה להקלטת אודיו.

5.5.1.22 בכול כניסה ויציאה מהמבנה יותקנו מצלמות טמ״ס לזיהוי הנכנסים והיוצאים.

5.5.1.23 בתכנון כניסת המבקרים יש לקחת בחשבון שער עבור כניסת נכים וכן דלפק נגיש לנכים לבידוק כנדרש.

5.6 מעגל פנימי: תכנון פנים כללי:

5.6.1 פירוט

5.6.1.1 ריכוזי קהל, בין אם אזורי קבלת קהל ובין אם אזורי המתנה, יתוכננו עד כמה שניתן באזור פנימי ללא קירות מסך/ קירות קלים בקרבתם ועם מינימום שטחי חלון בקירות חיצוניים הגובלים בריכוז הקהל חלונות אלו באזורי ריכוז הקהל ימוגנו כנגד הדף למניעת הפגעות המונית.

5.6.1.2 ארכיונים מרכזיים וחדרי תקשורת ומחשב נדרשים לקירות ודלתות מוגנים ולכן בשאיפה יבנו עד כמה שניתן בגרעיני המבנה עם קירות בטון מזוין ודלתות / חלונות מבוקרים ועמידים בפריצה אלימה (ראה פרק מפרט טכני).

5.6.1.3 נמחק לא רלוונטי לפרוייקט זה.

5.6.1.4 אזורי קבלת קהל גדולים ייבנו עד כמה שניתן בקומות הכניסה הראשית או קרוב אליה, ירוכזו באזור אחד תוך אפשרות מידור פשוט וקל של אזור קבלת הקהל משאר המבנה ותוך התחשבות באפשרות של אירוע ביטחוני וסדר ציבורי באזור זה, ריכוז הקהל ייעשה עד כמה שניתן רחוק מאזור הבידוק הביטחוני.

5.6.1.5 חדרי הממ"ק יתוכננו בהתאם לצרכי המשרד כדי שיוכלו לשמש חדרי מצב, דיונים ומחסה לקומה בה הם ממוקמים גם אם יחרגו בגודלם מהשטח המחייב ע"י פקע"ר.

5.6.1.6 לא רלוונטי לפרוייקט זה.

5.6.1.7 בקומת הקרקע או בסמיכות ישירה ללובי הכניסה הראשית יתוכנן אזור ביטחון שיכלול :חדר קב"ט (15 מ"ר, חדר ס.קב"ט (10 מ"ר), מזכירות (10 מ"ר), חדר בקרה (40 מ"ר), חדר ציוד לתקשורת (10 מ"ר), מחסן נשק (15 מ"ר), מחסן ביטחון לציוד (10מ"ר), חדר מאבטחים/מנוחה (25 מ"ר), שירותים (7 מ"ר), מטבחון (5מ"ר). יש לקחת בחשבון בשלב התכנון כי מוקד הבקרה צריך לעמוד כנגד איום הייחוס הרלוונטי קונבנציונאלי ובלתי קונבנציונאלי כך שיוכל להמשיך לתפקד גם בזמן חירום ללא צורך בפינוי בחירום המיקום של מוקד הבקרה וחדר הציוד של מוקד הבקרה יהיה במקום המוגן ביותר **<u>בתוך מתחם חדרי המצב</u>** ויאפשר שליטה מלאה על מכלול חדרי המצב גם בחירום וגם בשגרה .

5.6.1.8 יתוכננו בקרות פריצה במסדרונות, חדרי מדרגות וחדרים ספציפים תוך חלוקת מערכת בקרת הפריצה לאזורים מרובים כולל אזורי דריכה עצמאיים למקומות מסוימים עפ"י דרישת הקב"טים הרלוונטים ולכל הפחות בחדרי הקב"טים, חדר הנשק, לשכות שרים ואזורים מסווגים

מרמת סודי ומעלה.

5.6.1.9 מערכות באזורים מסווגים לסודי ומעלה- יותקנו באמצעי בקרה אלקטרונים עפ"י הנחיות שב"כ (נוהל ארץ), לפני תכנון וביצוע יובאו לאישור ולאחר הביצוע יש לעבור וועדת קבלה של השב"כ.

5.6.1.10 המערכת הפנימית תכלול מצלמות טמ"ס קבועות ומתניעות לכיסוי לוביים, כניסות למחלקות, חדרי מדרגות, אימות אזעקות באזורים ממודרים, דלתות מבוקרות מתוך מטרה לייעל את תהליך אימות האזעקות ובקרת הכניסה והכל באמצעות מערכת שו"ב.

5.6.1.11 תתוכנן רשת תקשורת TCP/IP יעודית לביטחון שתיבנה בטופולוגיית "כוכב" ותהיה בעלת שרידות גבוהה ביותר הכוללת לפחות שתי מתגי CORE המתאימים לנפחי התעבורה של כלל מערכות הביטחון אבזרי הקצה ועיבוד הנתונים עבור כלל מערכת הביטחון. כל ריכוזי הקצה יחוברו בסיבים אופטיים לכל מתגי ה CORE . ראה פרק "רשת תקשורת ייעודית לביטחון" בהמשך המסמך.

5.6.1.12 תתוכנן מערכת אינטרקום IP בין כניסות הראשיות לבניין, כניסות למחלקות,מעברים מבוקרים מעליות וחדר הבקרה הביטחוני, מערכת האנטרקום תהיה ייעודית לביטחון ותשתמש ברשת התקשורת הייעודית לביטחון המערכת תאפשר מיתוג אוטומטי של מצלמות בדלתות ומעברים מבוקרים והצגת התמונה בפנל השליטה לפתיחה קלה ויעילה – משולבת- אינטרקום, צפייה ולחצן פתיחה.

5.6.1.13 יתוכננו תשתיות ייעודיות למערכות הביטחון ורשת התקשורת לביטחון הכולל תעלות רשת, תעלות פח , פירים וצינורות יש לקחת בחשבון בתכנון תעלות הרשת והפח גידול עתידי של המערכות לפחות ב 20%.

5.6.1.14 תתוכנן פריסה של לחצני מצוקה ברחבי המתקן עפ"י דרישות הקב"טים הרלוונטים.

5.7 מעגל פנימי : מידור :

5.7.1 פירוט:

5.7.1.1 יש לקחת בחשבון בזמן התכנון שכל קומה במבנה תמודר באזור לובי המעליות באמצעות דלתות עמידות לפריצה קרה ומערכות בקרה. דלתות היציאה מפירי המדרגות יהיו מבוקרות גם הן באמצעות בקרת כניסה לצורך מידור פנימי, המידור ימנע כניסה בלתי מורשית הן בחדירה שקטה והן בפריצה אלימה למשך 5 דקות אל כל אחת מהאזורים הממודרים בבניין דלתות הכניסה הראשיות ליחידה יעמדו בפני פריצה אלימה ל 5-2 דקות לפחות

5.7.1.2 יש להתייחס בזמן התכנון האדריכלי לאפשרות מידור פיזי וטכנולוגי של אזורים מסווגים בתוך המשרדים בהתאם להנחיות סגן ר' מערך סייבר חירום וביטחון במשרד האוצר וגופי הביטחון וחלוקה בין

משרדים ומדורים שונים באותם המשרדים. יש לחשוב על פתרון אדריכלי שיפשט את נושא בטיחות האש, תפעול יום יומי תוך צמצום עלויות במקרה של צורך במידור כנ"ל בין או בתוך קומות משרדים.

5.7.1.3 יש לקחת בחשבון כי מידור בתוך קומות יכול להשפיע על מיקום שירותים, צרכי מיזוג אוויר, בטיחות אש ועוד- תכנון נכון ואפקטיבי יחסוך כסף רב.

5.7.1.4 יש לייצר מידור בין השטחים המסחריים והחניונים לקומות המבנה זאת בכדי לוודא כי אדם המבקש להכנס למתקן יהיה מחוייב לעבור תחילה דרך מערך הבידוק בלובי הראשי של המתקן.

5.7.1.5 יש לקחת בחשבון כי בכניסה למקומות מסווגים או בכניסות המובילות מהחניון למתקן עצמו יותקנו מערכות טכנולוגיות ופיזיות למניעת הסתננות של מבקרים.

5.8 מעגל פנימי: חדר בקרה:

5.8.1.1 מוקד בקרה ביטחוני יאפשר שליטה, בקרה ושליטה מלאה על מערכות הביטחון ומערכות בקרת המבנה בכל זמן נתון וללא צורך לצאת מהחדר הן בשגרה והן בחירום כולל ניהול אירוע רב משתתפים ותגבור כ"א.

5.8.1.2 מערכות הביטחון ובקרת המבנה יעבדו בממשק מלא האחד עם השני.

5.8.1.3 הממשקים בין מערכות הביטחון יהיו ברמת IP ויכילו את כל הפונקציונאליות המתאפשרת מה SDK של כל תת מערכת.

5.8.1.4 מוקד הביטחון ינוהל ע"י מערכת שו"ב ומולטימדיה כולל קיר ווידאו מתקדמת היכולה לנהל מספר אירועים שונים במקביל ואשר מקבלת אינפורמציה בממשק מלא ממערכות הבטיחות ובקרת המבנה וכן יכולה להזין ולקבל נתונים ממערכות חיצוניות רחוקות מהמתקן, יודגש כי לא תתאפשר שליטה מרחוק על מערכות אלו לצורך טיפול מונע ו/או לצורך תיקון המערכות. יחד עם זאת המזמין רשאי לאפשר תיקון תקלות בתתי המערכת מרחוק וזאת בהתאם לנהלי עבודה ומערכות בקרה שיותקנו באישור המזמין בלבד (הנ"ל מתייחס לכלל המערכות האלקטרו מכאניות שיותקנו במתקן) .

5.8.1.5 מוקד הביטחון ימוקם באזור המוגן ביותר במבנה ,בתוך מתחם הביטחון, וייבנה בהתאם לאיום הייחוס העדכני ולעמידה כנגד אירוע קונבנציונאלי וכן יכלול מערכות סינון אקטיביות בהתאם לתקן פקע"ר באופן שיאפשר תפקוד מלא מהמקום בעת אירוע אב"כ.

5.8.1.6 פירוט דרישות מלא של חדר הבקרה הביטחוני יעשה עפ"י האמור בפרק המפרט הטכני במסמך זה ויאושר ע"י סגן ר' מערך סייבר חירום וביטחון במשרד האוצר.

5.8.1.7 יובהר כי המוקד בבניין זה יחובר בעתיד למוקד הארצי (ג'נרי 2)

במסגרת פרוייקט "מערכת שו"ב ארצית לביטחון – PCIM-Physical security information management". היזם מתחייב לספק את כל מסמכי ה SDK וה API של כלל מערכות הביטחון לטובת יישום פרוייקט "מוקד ארצי לביטחון" ולשתף פעולה בכל הדרוש ליישום פרוייקט זה. על היזם לבצע את ההכנות הדרושות לחיבור רשת התקשורת הארצית לביטחון בארון התקשורת המרכזי של הבנין.

5.9 מעגל פנימי : חניונים:

5.9.1 פירוט:

5.9.1.1 לא רלוונטי לפרוייקט זה.

5.9.1.2 חניון הבניין נדרש להיות עבור עובדי הממשלה בלבד. חובה לתכנן את מערך המעליות וחדרי המדרגות העולות ממנו כך שיצאו באזור ציבורי (מחוץ לבניין) או מחוץ לאזור הבידוק הביטחוני (לובי כניסה ראשי).

5.9.1.3 מיגון החניון כנגד התפרצות יעמוד כנגד איום הייחוס של הגופים המנחים באמצעות מחסומי נגיפה לפחות ברמה של 4K עפ"י התקן האמריקאי , בכלל זה כנגד רכב מתפרץ אופנועים וחדירת הולכי רגל בלתי מורשים לחניון, יש לתכנן בקרת כניסה מלאה לחניון באמצעות מערכת lpr וכן מערכות טמ"ס ובקרת כניסה , יש לתכנן נתיב סירוב גישה לרכב כך שניתן יהיה לסובב רכב בלתי מורשה ללא כניסה למתחם החניון, תתוכנן סגירת לילה מלאה למתחם החניון שתמנע חדירה לשטח החניון באמצעות מחסומים פיזיים ומערכות גילוי ותצפית אלקטרוניים, כל פיתרון אדריכלי יוצג לאישור סגן ר' מערך סייבר חירום וביטחון במשרד האוצר לפני אישור ביצוע.

5.9.1.4 הפעלת החניון שלא בשעות העבודה ובסופי השבוע – במידה ויאושר למפעיל החניון מתן שרותי חניה בשטחי החניון בשעות שאינן שעות הפעילות הסטנדרטיות של המשרדים ובסופי השבוע ימשיך החניון להיות מאובטח באמצעות יחידת הבטחון של הקריה בהתאם לרמת האבטחה שיגדיר קב"ט הקריה, עלויות אלו של אבטחת החניון יכולו על היזם/מפעיל החניון באופן ישיר.

5.9.1.5 אבטחת החניון – האבטחה בחניון הינה חלק בלתי נפרד מאבטחת המבנה והקומפלקס ועל כן מערך האבטחה של המתחם ייתן מענה גם לחניון ויהיה חלק בלתי נפרד מיחידת הביטחון של המבנה, מאבטחי החניון יהיו חלק מכוח האבטחה של המבנה ויהיו כפופים ישירות לקב"ט המבנה הממשלתי עלויות אבטחת החניון יכולו על היזם/מפעיל החניון בהתאם להגדרות ודרישות הביטחון שיוגדרו על ידי מערך סייבר חירום וביטחון במשרד האוצר .

5.10 מעגל פנימי: מעליות:

5.10.1 פירוט:

5.10.1.1 המעליות המתוכננות לבניין יהיו מסוג המאפשר שימוש באמצעי מידור כגון בקרות כניסה ואמצעי בקרה פנימית באמצעות מצלמת טלוויזיה במעגל סגור וקוראי כרטיסים.

5.10.1.2 במעלית יהיה אינטרקום המאפשר דו שיח בין הנמצא במעלית וחדר הבקרה הביטחוני ובקרת המבנה, ייזום שיחה דו סתרי.

5.10.1.3 לוחות בקרת המעליות ימוקמו בחדר בקרת מבנה/ אב בית , וגם בחדר הבקרה הביטחוני, תהיה יכולת שליטה מלאה בתפקוד המעליות מחדר הבקרה הבטחוני .

5.10.1.4 לא רלוונטי לפרוייקט .

5.11 מעגל פנימי: מיזוג אוויר:

5.11.1 פירוט:

5.11.1.1 למערכת מיזוג אויר תתוכנן חלוקה פנימית אשר תאפשר סגירת אזורים שונים בבניין באופן פרטני, בשאיפה כל קומה, לצורך בידוד אזור בעייתי או שנפגע.

5.11.1.2 שליטה על הפעלה וכיבוי כלליים של המערכת תהיה במקביל בחדר הבקרה הביטחוני בנוסף לחדר בקרת מבנה.

5.11.1.3 פתחי כניסת האוויר יתוכננו באזור לא נגיש משטחים ציבוריים, ברוב המקרים יהיו המערכות על גג המבנה. גם אז יהיו אזורים אלו סגורים, נעולים ומבוקרים כנגד כניסת בני אדם לא מורשים ובאמצעי גילוי אלקטרוניים.

5.11.1.4 בנקודות מרכזיות במערכת המיזוג אוויר יותקנו גלאים אשר יוכלו לזהות חדירת חל״כ ו/או ביולוגי למערכת כמו כן יותקנו מנורות אולטרה סגול לטיהור וחיטוי אוויר בתעלות המיזוג.

5.11.1.5 מיזוג האוויר בחדרי השרתים וחדרי הבקרה יהיו ממוגנות כנגד איום הייחוס על כל רכיביהן כולל הצ׳ילרים, נדרשת יתירות מלאה למערכות המיזוג לחדרים אלו אשר ימוקמו באזורים נפרדים ממערכות המיזוג המרכזיות.

5.12 כללי: חשמל:

5.12.1 פירוט:

5.12.1.1 מלבד כל האמור בהמשך לגבי מערכות המתח הנמוך מאוד בבניין, יש לוודא בתכנון החשמל את המצאות העקרונות הבאים :

5.12.1.2 כל מערכות הביטחון יחוברו לרשת חשמל החירום של הבניין כולל UPS וגנרטור ויעמדו בכל דרישות היתירות המקסימאליות שהוגדרו לחדרי המצב במבנה.

5.12.1.3 בכל קומה יתוכנן ארון ריכוז בעל יכולת נעילה ובקרה לכל מערכות האבטחה, שימוקם בחדר התקשורת הקומתי.

5.12.1.4 תכנון התאורה בבניין יאפשר שליטה על תאורת חוץ ולובביים ממוקד הביטחון .

5.12.1.5 בהיקף הבניין ובלובביים הציבוריים תתוכנן תאורה אשר תסייע למערכת הטמ״ס ברמה של 2 לוקס ממוצע בשטחים חיצוניים פתוחים ו 5 לוקס ממוצע בשטחים פתוחים פנימיים.

5.12.1.6 יתוכננו פנסי תאורה היקפיים מסביב כל הבניין שיופעלו על ידי גלאי תנועה .

5.12.1.7 חדרי השנאים הגנרטורים ומערכות ה UPS של המבנה יהיו ממוגנים כנגד איום הייחוס .

5.12.1.8 נדרשת יתירות מלאה לכל הרכיבים הקריטיים במבנה המערכות ליתירות ימוקמו באזור נפרד מהמערכת הראשית.

5.12.1.9 נדרשים מכלי סולר ממוגנים ויתירים עבור הגנרטורים, עם כמות סולר שתספיק לעבודה רציפה של המבנה לפחות ל72 שעות.

5.12.1.10 על מתכנן החשמל לקרא בעיון את פרקי מערכות האבטחה ולהתייחס אליהם בתכנון התשתיות בבניין.

5.12.1.11 חדרי החשמל UPS וגנרטור ימוגנו באמצעי בקרת כניסה וגילוי אלקטרוניים וימוקמו באזורים ללא גישה חופשית של אזרחים. דלתות הכניסה למתחמים אלו יהיו עמידות לפריצה לפחות לחמש דקות עם מערכות בקרת כניסה ונעולות.

5.13 כללי: תקשורת: וחדר מחשב מרכזי

5.13.1 פירוט:

5.13.1.1 כלל התשתיות של מערכות הביטחון יוגדרו כתקשורת אדומה ועל כן התשתית לכלל המערכות הללו יבנו בהתאם לדרישות תקשורת אדומה ובהתאם להנחיות הגופים המנחים ולדרישות סגן ר׳ מערך סייבר

חירום וביטחון במשרד האוצר. יש לקחת בחשבון כי כלל התקשורת תרוץ בתוך תעלות פח ואמצעים העומדים במיגון תקשורת אדומה.

5.13.1.2 יש להתחשב בכך שיינתנו הנחיות למערכות תקשורת ייחודית לאזור הביטחון כמוגדר בפרק הנחיות התכנון בהמשך.

5.13.1.3 יש לתכנן הטלפוניה באופן שהמרכזייה תאפשר התקנת יחידות פנקוד לתפקוד כאינטרקום , הפנקודים ימוקמו בכניסה למשרדים בלובי המעליות ובמקומות נוספים אשר יוגדרו מראש.

5.13.1.4 חדר תקשורת מרכזי : יש לתכנן חדר תקשורת מרכזי שימצא בקומה תת קרקעית. החדר יהיה מוגן כנגד איום הייחוס העדכני בתקן של רמת המיגון המקסימלית שהוגדרה למתקן .

5.13.1.5 בכל קומות חניון או מחסן תת קרקעיות, יש להתקין אינטרקומים לצרכי הביטחון בקומות אלו .

5.13.1.6 רשתות תקשורת ייעודיים לביטחון (רשת אדומה אחת לפחות) עפ״י אפיון של סגן ר׳ מערך סייבר חירום וביטחון במשרד האוצר.

5.13.1.7 כל מערכות התמך של חדר המחשב והתקשורת המרכזי של המבנה תהינה מוגנות ויתירות (מיזוג, חשמל, גנרצייה, UPS) .

5.13.1.8 בחלל חדר המחשב תהיה הפרדה בין הגופים השונים באמצעות כלובים מוגנים ונעילות שישמשו אך ורק את המורשים מטעם המשתמש הסופי ללא יכולת נגישות של אף גורם אחר בלתי מורשה.

5.1 הגנה בפני התקפות סייבר :

במסגרת העבודות יוגדרו ליזם דרישות נוספות הקשורות להגנה בפני התקפות סייבר הכוללות הן הנחיות בתחום האבטחה והליווי הנדרש במסגרת תהליך הקמת הפרוייקט בדגש על אזורים בעלי רגישות גבוהה (כגון חדרי מחשב, תקשורת , בקרה, גנרציה, חשמל טלפוניה וכו׳) והכל כמפורט בנספח 9 המצ״ב.

5.1.1.1 רכש מבצעי :

5.1.1.2 ינתנו הנחיות לביצוע במסגרת פעולות הרכש של היזם עבור הפרוייקט הכוללות בין היתר הנחיות כיצד לבצע את הרכש עבור רכיבים מסויימים לפרוייקט בדגש על המערכות האלקטרו מכאניות היזם מחוייב לתת מענה לדרישות אלו ולהציג את השיטה לאישור הגורם המקצועי במערך סייבר חירום וביטחון במשרד האוצר.

5.1.1.3 היזם יציג תכנון מלא לרציפות תפקודית של כלל המערכות המוגדרות כמערכות חיוניות לתפקוד המתחם והמבנה בחירום ברמת N3 עבור מערכות הביטחון בקרת המבנה מערכות הבטיחות וחדרי המצב של המבנה ומכלולים רגישים שיוגדרו על ידי המזמין.

5.1.1.4 היזם יעמיד יועץ לרציפות תפקודית ויועץ להגנה בפני התקפות סייבר ברשימת היועצים לאישור מערך סייבר חירום וביטחון במשרד האוצר , היועץ יהיה בעל נסיון קודם בהקמת מערכות המצריכות רציפות

תפקודית והגנה בסייבר במערכת הביטחון (צה"ל , מוסד, שב"כ).

5.1.1.5 הנחיות נוספות יינתנו ליזם במהלך התכנון הראשוני והמפורט על היזם להציג את המענה לדרישות אלו באמצעות יועצים לרציפות תפקודית והגנה בסייבר ויאושרו על ידי נציג מערך סייבר חירום וביטחון במשרד האוצר .

5.1.1.6 בידוק ביטחוני לעובדי היזם הקבלן המבצע וחברות התחזוקה נותנות השרותים : היזם מחוייב לשתף פעולה בכל הקשור לביצוע בדיקות ביטחון למועסקים בפרוייקט זה הן במסירת המידע ,חתימה על טפסים וכן הפסקת מתן השרותים באמצעות גורם כזה או אחר במהלך הקמת הפרוייקט ו/או במסגרת מתן שרותי התחזוקה לאחר מסירת הפרוייקט.

5.1.1.7 חתימה על סודיות ושמירה על מסמכים :

5.1.1.7.1 היזם מחוייב לחתום על מסמכים שיועברו לחתימתו או לחתימת מי מעובדי היזם הקבלן היועצים האדריכלים וכו' בכל הקשור לשמירת סודיות .

5.1.1.7.2 היזם מתחייב להרחיק כל גורם אשר יסרב לחתום או ימנע מלשתף פעולה עם מערך הביטחון של משרד האוצר בנושא זה.

5.1.1.8 שמירה על מסמכים תוכניות ומידע : באחריות היזם לבצע את כל הפעולות הנדרשות בכדי למנוע זליגת מידע שיוגדר במסגרת הפרוייקט כמידע רגיש ביטחוני בכל רמה שהיא לגורם בלתי מוסמך וכן למדיה שאינה מאושרת (אינטרנט למשל) בכל הקשור למסמכים שיועברו ליזם או ליועצי היזם או לעובדי הקבלן וכו' כמו כן יוגדרו חלק מהתוכניות כתוכניות רגישות אשר פרסומן עלול לפגוע בביטחון המתקן והמידע על היזם לפעול בהתאם להנחיות הביטחון שינתנו לו מעת לעת על ידי מערך סייבר חירום וביטחון במשרד האוצר והוא מתחייב לפעול על פיהן.

5.1.1.9 ביצוע עבודות רגישות בתוך המתחם :
יוגדרו ליזם משימות ועבודות במהלך הקמת הפרוייקט אשר עקב רגישותם יבוצעו בתוך המתקן תחת אבטחה או ליווי. באחריות היזם לדאוג לא לבצע עבודות אלו ללא עדכון מוקדם של הגורם המצועי מתאם מערך סייבר חירום וביטחון באוצר וכן להציב את האמצעים הנדרשים בכדי לאפשר הגנה על מתחמים אלו לאחר התקנת חלק מהציוד (באופן זמני עד למסירת המתקן).

5.1.1.10 חובת דיווח על אירוע אבטחת מידע - על הקבלן לדווח בכל מקרה של חשש לאירוע בתחום א. המידע אצלו ואצל כלל קבלני המשנה היועצים ונותני השירותים השונים , היזם מתחייב לאפשר ביקור של גורמי א. המידע של המזמין וביצוע תדרוך לעובדים בפרוייקט.

5.1.1.11 התקנת מערכות לניתור רשתות הביטחון והתראה על שינוי ו/או חיבור לנקודות תקשורת כדוגמת sayber switch, היזם ידרוש ממתכנני מערכות האלקטרו מכאניות במסגרת מכרזי הרכש לפרוייקט כי

החברות יבצעו מערכות העומדות בדרישות ההגנה בסייבר וכוללת מערכות לזיהוי ואיתור חריגים בכל הקשור לרשתות בקרת המבנה בקרת הביטחון מערכות רגישות אחרות בבניין עפ״י הגדרת נציג מערך סייבר חירום וביטחון במשרד האוצר (מניעת שליטה מרחוק וטיפול מרחוק בכפוף להנחיות המזמין וחיבור מערכות בקרה וניטור) .

5.1.1.12 כמו כן במסגרת הגשת תוכניות לאישור יציגו המתכננים תוכניות הכוללות את כלל הרכיבים התוכנות וההגנות המתוכננות למערכות הבניין ומערכות המיחשוב והתקשורת לאישור מערך סייבר חירום וביטחון.

5.2 כללי: בטיחות:

5.2.1 פירוט:

5.2.1.1 יש לבצע תיאום בין יועץ הבטיחות ליועץ הביטחון כבר בשלב התכנון הראשוני כדי למנוע התנגשויות בנושאי אש וכדומה.

5.2.1.2 במידה וישנו חניון ציבורי או כל אזור ציבורי אחר יש לתכנן ממנו מדרגות מילוט החוצה ולא לתוך האזור המוגן של המבנה.

5.2.1.3 יש לתאם את נושא פתיחת דלתות המילוט לשטחים ציבוריים רק לאחר השהייה והקפצת תמונות ממערכת הטמ״ס כבר בשלב נסיון הפתיחה הראשוני (לחיצה על קרש בר או לחצן שבירה)

5.2.1.4 יש לתכנן את הפירים השונים של התשתיות באופן נפרד כך שבעת נזק לאחד מהם לא יופרעו האחרים .

5.2.1.5 על הקבלן המבצע לדאוג לפריסה של שילוט מלא במתקן הכולל שילוט יציאה לחירום והכוונה לממ״קים.

5.3 הנחיות לתפעול שוטף ותחזוקה:

5.3.1 פירוט:

5.3.1.1 במידה ויש צורך בהכנסת סחורות לבניין, אם לצורך תפעולו השוטף של הבניין ואם לצורך שטחי מסחר, שכנים הקיים בו, יש לשאוף לאפשר הכנסת הסחורות ללא כניסת המשאיות לחניון תת קרקעי או לאזורים רגישים, ולאפשר ציר תנועה של עגלות למעליות השרות – כדי למנוע הצורך בבידוק בטחוני ארוך ויקר.

5.3.1.2 יש לתכנן תמונת ראי של מערכת בקרת המבנה במוקד הביטחון באמצעות קליינטים למערכת בקרת המבנה והאש הטיפול על ידי טכנאי המערכת ואנשי התחזוקה במערכת ייעשה בחדר התחזוקה ולא

במוקד הבקרה הבטחוני לא תתאפשר תחזוקה מרחוק למערכות בקרת הביטחון בקרת המבנה אש ובטיחות וכן למערכות אלקטרו מכאניות אחרות המותקנות במבנה ללא אישור מראש ובכתב של קב״ט המבנה ובכפוף לעמידה בהנחיות המזמין למתן תחזוקה מרחוק עפ״י נהלי העבודה והתקנת מערכות בקרה שיוגדרו על ידי קב״ט המתקן.

5.4 חירום / פקע״ר חדרי פיקוד

5.4.1 פירוט:

5.4.1.1 אזורי המיגון המחויבים בחוק יתוכננו בהתאם לצורך המעשי של המשרדים לאיוש ופעולות בחרום לאומי מתמשך ולא לפי המינימום הנדרש ע״י פקע״ר.

5.4.1.2 במהלך התכנון האדריכלי יתבקשו המשרדים השונים להגדיר האם ישנם חדרים נוספים (לשכות, חדרי פיקוד, וכד׳) אשר נדרשים להיות מוגדרים כממ״קים עם מערכות סינון. באחריות העונים על מפרט זה לקחת בחשבון תוספת של מספר חדרים כאלו בזמן התמחור.

5.4.1.3 יש לוודא קיום או התאמת אזורים בהגדרה ״הכי מוגן שיש״ , כלומר, אזור פנימי ללא חלונות אשר אינם קומה עליונה ואינם פונים בחזית חשופה לאזור איום עיקרי.

5.4.1.4 גודל אזורי המיגון הנדרשים יתוכנן עם דיירי המשרדים והדיור הממשלתי עפ״י כמות האנשים הצפויים ואופי הפעילות הצפויה בעת חירום. תתוכנן במקום תשתית לכמות עמדות עבודה מקסימאליות .

5.4.1.5 ממ״קים לשימוש הנמצאים באזורים ציבוריים, יהיו נגישים מהאזור הציבורי ללא מעבר דרך אזור מוגן וללא אפשרות למעבר לא מבוקר מהממ״ק לאזור הפנימי.

5.4.1.6 בבניין תותקן מערכת ״דיווחית״ של חברת ביפר להתראה על מצבי חירום ע״י פקע״ר.

5.4.1.7 במידה וישנם ממ״קים אשר מותקנים על דלתותיהם מערכות בקרת כניסה אלקטרוניים, יש לוודא אפשרות ניתוקם ופתיחת הדלתות מחדר הבקרה הביטחוני .

5.4.1.8 בבניין תותקן מערכת לזיהוי מקדים של רעידת אדמה (עפ״י מפרט טכני בפרק מתח נמוך).

5.4.1.9 על הקבלן לרכוש ולהתקין מערכות קשר מרכזית בבניין שתשמש את מערך האבטחה במקום וזאת עפ״י המפרט הטכני כולל ביצוע אנטנות על הגג כנדרש.

6 מיגון פיזי- המפרט הטכני

6.1 היקף הבניין

6.1.1 פירוט:

6.1.1.1 בהיקף המתקן תתוכנן חסימת רכב שתמנע חדירת רכב בלתי מורשה בכל מצב אם בכוח, אם בתחבולה ואם באמצעים טכניים, דרך חסימה זו. החסימה תתבצע על גבול המגרש ורחוק עד כמה שניתן מקיר המבנה או נקודות קריטיות בו. החסימה יכולה להתבצע ע"י עמודי פלדה, חגורות בטון, מדרגת קרקע, מסלע או כל אמצעי אחר ובתנאי שיעמוד ברמה זהה לתקן עמידה כנגד רכב מתפרץ ברמה K-4 (לפי תקן משרד החוץ האמריקאי) לפחות בהתאם לניסוי או לחישובי מהירות ואנרגיות שיגיש יועץ המיגון והאבטחה לאישור סגן ר' מערך סייבר חירום וביטחון במשרד האוצר לפני תכנון מפורט.

6.1.1.2 חסימת הרכב ההיקפית תבוצע באופן רציף ובכל מקרה המרחק בין חלקי המחסום לא יעלה על 110 ס"מ וגובהו לא יפחת מ- 60 ס"מ

6.1.1.3 במקביל וללא קשר לנ"ל יידרש גם גידור / קיר מגן לצורך סימון גבולות המתחם ועצירת כניסת הולכי רגל מלהיכנס באופן חופשי אל המתחם. הגידור ההיקפי יהיה בגובה מינימאלי של 280 ס"מ ומתוכנן בהתאם לתקנים וההנחיות המחמירות של משטרת ישראל במבני ציבור. בנוסף, יהיה הגידור ההיקפי מואר באופן מספק לצורך תפעול יעיל ונוח של מצלמות ביטחון שיותקנו בהיקף המתקן ברמת תאורה ממוצעת של 2 לוקס לפחות.

6.2 כניסות

6.2.1 פירוט:

6.2.1.1 שערי רכב יתוכננו ויבנו בהתאם לרמת המיגון של הגדר ההיקפית – ברמה K-4 לפחות (לפי תקן משרד החוץ האמריקאי) בהתאם לחישוב ותכנון של יועץ המיגון והאבטחה כנ"ל.

6.2.1.2 בזמן תכנון מחסום הרכב יילקחו בחשבון הנושאים הבאים:

6.2.1.3 מחסום יכול להיות מחסום זרוע נגד התפרצות או עמודי חסימה מתרוממים או כל מחסום אחר. בהנחה כי עומדים בדרישות התקן (K-4 ומעלה), עונה לדרישות המיגון, עונה לצרכי הבטיחות והתפעול של הבניין.

6.2.1.4 על נקודת החסימה להיות בנקודה המרוחקת ביותר האפשרית מן

הבניין.

6.2.1.5 בתכנון התנועה יילקח בחשבון כי רכב שיעמוד לפני השער ייבדק עד מספר דקות – רצוי לאפשר שני נתיבים או יכולת עקיפה לרכב מורשה.

6.2.1.6 תתאפשר פניה של רכב מסורב כניסה ללא הכרח בהכנסתו למתחם לצורך כך אזור הבידוק יתוכנן כמקום נוח ומוגן משמש, רוח וגשם לפחות לאיש האבטחה ואמצעי השליטה על השער.

6.2.1.7 מערך הכניסה יכלול חבילת אמצעי בטיחות מלאה כולל רמזורים לולאות כביש וגלאי מעבר רכב.

6.2.1.8 תידרש סגירת לילה הרמטית באמצעות שער נגרר או תריס גלילה עמיד בפריצה אלימה .

6.2.1.9 כל שער רכב יהיה מבוקר ונשלט מחדר הבקרה בבניין ויאפשר גם כניסה ויציאה באמצעות בקרת כניסה ממוחשבת הכוללת מערכת LPR.

6.2.1.10 מהירות הפתיחה והסגירה של השער תהיה עד 4 שניות. פתרון איטי יותר ניתן להגיש במידה ולא מתוכננת תנועה רבה בשער ובאישור המזמין

6.2.1.11 על המערכת המותקנת להיות של חברה מוכרת בתחום מחסומי הביטחון אשר התקינה מערכות כנ"ל בעבר לגופים ממשלתיים ופעילה בתחום לפחות 10 שנים.

6.2.1.12 על החברה להציג ניסויים או חישובים מוסמכים של ביצועי החסימה ברמה הנדרשת.

6.2.1.13 נדרש להתקין אמצעים להקטנת מהירות בדרך הגישה לשער הרכב .

6.2.1.14 פירוט לוגיקת ההפעלה תיעשה בסמוך להקמת המערכת יחד עם סגן ר' מערך סייבר חירום וביטחון במשרד האוצר.

6.2.1.15 ניתן לשלב בין שער הרכב הביטחוני לבין שערי ניהול חניון רק לאחר אישור והתייחסות ספציפית של המזמין .

6.2.1.16 במקרים מסוימים יתכן ויידרש גם שער כניסת הולכי רגל (בשגרה או בשעות הלילה) במקרה זה יעמוד השער באותן דרישות מיגון זהות לגדר / קיר אותם הוא ממשיך.

6.2.1.17 יש לקחת בחשבון בשלב התכנון בניית עמדת שומר מוגנת כנגד התפרצות ל15 דקות וכן כנגד ירי לפחות עד לגובה של 1.2 מ' הכוללת יכולת שליטה על מערכות הכניסה לחניון מערכת הזמנת מבקרים ותקשורת אל מול מוקד הבקרה .

6.3 חצרות היקפיים ופנימיים:

6.3.1 פירוט:

6.3.1.1 תכנון החצרות כולם ייקח בחשבון גם את שיקולי האבטחה תוך הימנעות עד כמה שניתן מיצירת שטחים מוסתרים בקרבת קירות המבנה או הגידור ההיקפי, יש להימנע משטחים שיאפשרו הסתתרות גורמים עוינים או מטענים חשודים בסבך הצמחייה ויקשו על סריקות מקדימות.

6.3.1.2 מיקום מכלי חומרים דליקים / מסוכנים, מצבורי אשפה וציוד יתבצע תוך התייחסות לשיקולי מיגון ואבטחה וקבלת חוות דעתו של יועץ האבטחה של המתקן ואישור הקב"ט.

6.3.1.3 תשתיות ניקוז, תעלות תשתית תת קרקעיות וכדומה, שמתחברות למערכות העירוניות ויוצאות את גבולות המתקן יתוכננו תוך התייחסות גם לשיקולי מיגון ואבטחה ומחייבות חוות דעת והמלצות יועץ האבטחה של הפרויקט ואישור הקב"ט.

6.4 הנחיות תכנון אמצעים במעטפת המבנה:

6.4.1 פירוט:

6.4.1.1 ככלל, מומלץ ביותר כי כל קירותיו החיצוניים של המבנה והפתחים שבו ייבנו כבניה קשיחה או מוגנת שתצמצם ככל הניתן את הנזק הישיר למבנה ותצמצם את כמות הנפגעים בהתרחש איום הייחוס כנגד המושא המאובטח.

6.4.1.2 על מנת שקיר ייחשב לבנוי מוגן מספיק ללא צורך בבחינה נוספת נדרשת בניה מבטון מזויין (כדוגמת קיר ממ"ד) בעובי 200 מ"מ לפחות עד קומה 5 ובלוק בטון עם חגורות קשורות או שווה ערך מקומה 6 ומעלה.

6.4.1.3 בניה מאלמנטים קלים יותר, (בלוקים, מסך זכוכית, בנית אבן קלה, וכדי) אפשרית, אך תדרוש מפרטי חיזוק / בניה מיוחדים שייקחו בחשבון את האיומים השונים כפי שיחושבו ע"י יועץ המיגון של היזם ואושרו ע"י הקב"ט.

6.4.1.4 אלמנטים טרומיים מותרים ובתנאי שיתבצעו חיבורים מתאימים לעומסים המקסימאליים הצפויים כתוצאה מפיצוץ ושיאושרו ע"י יועץ המיגון / קונסטרוקטור הפרויקט.

6.4.1.5 כל פתחי המבנה – דלתות וחלונות מקבלות התייחסות נפרדת – ראה בהמשך.

6.4.1.6 חיזוק קיר חיצוני נגד פריצה (כולל הפתחים : חלונות ודלתות) –

6.4.1.6.1 יידרש בכל היקף המבנה מהקרקע – או מקום עמידה נוח ונגיש

לציבור, ועד לגובה של קומה שלישית לפחות ממשטח העמידה.

6.4.1.6.2 מכלול הקיר והחיבורים יתוכנן לעמוד בפריצה אלימה של המון מתפרץ למשך 15 דקות לפחות בהתאם לשיטות וחומרים מאושרים ע"י תקן רלוונטי או ניסוי מאושר ע"י סגן ר' מערך סייבר חירום וביטחון במשרד האוצר. דוגמה לפתרון כנ"ל – קיר בטון מזוין (מפרט ממ"ד) בעובי 20 ס"מ לפחות.

6.4.1.6.3 פתחים בקיר חיצוני יעמדו בדרישה זהה – ראה פרוט בהמשך.

6.4.1.7 חיזוק קיר באזורים מיוחדים (קיר חיצוני או פנימי) כנגד פריצה יידרש לפחות באזורים הבאים:

6.4.1.7.1 חדר נשק – יבוצע בהתאם למפרט משטרת ישראל הרלוונטי ואישור המשטרה.

6.4.1.7.2 ארכיונים מרכזיים מסווגים – יעמדו בפרטי היחידה לאבטחת מידע ברמת סודי (עמידה חמש דקות לפחות בפני פריצה אלימה וסמויה) ויאושרו ע"י סגן ר' מערך סייבר חירום וביטחון במשרד האוצר.

6.4.1.7.3 חדר משרד ברמת סודי ומעלה – יעמוד בפרטי היחידה אבטחת מידע ברמת סודי (עמידה חמש דקות לפחות בפני פריצה אלימה וסמויה) ויאושרו ע"י סגן ר' מערך סייבר חירום וביטחון במשרד האוצר.

6.4.1.7.4 לשכת שר / אח"מ מאויים – יעמדו בדרישות המיגון של יחידה לאבטחה אישים (עמדה של 5 דקות בפריצה אלימה) ואישור קב"ט המשרד הרלוונטי.

6.4.1.7.5 אזור מח' הביטחון – יעמדו בדרישות מידור בסיסיות ובמידה וממוקמים בקומת הקרקע או אזור פתוח לציבור גם בפני פריצה אלימה למשך 5 דקות לפחות לפי תקן רלוונטי ו/או אישור יועץ המיגון סגן ר' מערך סייבר חירום וביטחון במשרד האוצר.

6.4.1.7.6 חדרי תקשורת – יעמדו בדרישות מידור ופריצה אלימה בסיסיות ברמת "פלדלת" וקיר לבנים ישראליות בעובי 10 ס"מ עם חגורות קשורות או שווה ערך.

6.4.1.7.7 חדרי מחשבים – יעמדו בדרישות מידור ופריצה אלימה בסיסיות ברמת "פלדלת" וקיר לבנים ישראליות בעובי 10 ס"מ עם חגורות קשורות או שווה ערך. בכל מקרה יקבל כל חדר מחשב הנחיה ואישור בכתב לרמת המיגון מטעם קב"ט המשרד הרלוונטי.

6.4.1.7.8 אזורים ממודרים כפי שיוגדרו ע"י הקב"טים הרלוונטיים – רמת מיגון פרטנית כפי שתתקבל מהקב"ט ובהתאם להנחיתו.

6.4.1.7.9 כל אזור ממודר מסיבות ביטחונית יקבל מיגון מעטפת ברמה

שלא תפחת מ : בבלוק ישראלי בעובי 100 מ״מ וחגורות קשורות או פלטות פלדה עובי 2 מ״מ עוגנות לקונסטרוקציית פלדה לרצפה ולתקרה.

6.4.1.8 דרישות חיזוק קיר חיצוני נגד איום הדף יידרש לפחות באזורים הבאים :

6.4.1.8.1 כל קירות המבנה ידרשו התייחסות עמידות כנגד הדף פיצוץ (ע״פ איומי הייחוס המוגדרים ע״י מערך סייבר חירום ובטחון לקריות הממשלה) כפי שיחושב ע״י יועץ המיגון ויוגש על ידו, בשלב ניתוח הסיכונים ותוכנית המיגון והאבטחה (שלב ראשון בפרויקט המיגון). אמצעי המיגון כנגד הדף תבססו על שיטות שנבחנו ע״י פקע״ר או ארגון דומה עבור מבנה קיים או שיפור בניה ולאחר הצגת ניסויים להוכחת השיטה, תוכנית זו כולל החישובים וסקיצות ממוחשבות יוגשו לאישור סגן ר׳ מערך סייבר חירום וביטחון במשרד האוצר.

6.4.1.8.2 פתחים בקירות חיצוניים (דלתות וחלונות) יקבלו טיפול זהה – ראה בהמשך.

6.5 עקרונות תכנון לובי כניסה ראשי:

6.5.1 פירוט:

6.5.1.1 לובי כניסה יתוכנן כך שיאפשר בידוק מלא של האורחים הנכנסים הן ידני והן באמצעים טכניים שמשתנים לאורך השנים ומצד שני יאפשר כניסת עובדים תוך שימוש בבקרת כניסה ממוחשבת.

6.5.1.2 שטח הרצפה הנדרש יתוכנן עפ״י כמות הנכנסים והזמן הנדרש למעבר הבידוק או בקרת הכניסה אך תוך התייחסות למשקל הציוד הביטחוני ושטח הרצפה לה הוא ניזקק :

6.5.1.2.1 מינימום שטח רצפה למכונת שיקוף 100X300 ס״מ

6.5.1.2.2 מינימום שטח ריצפה לשער מגלה מתכות 130X130 ס״מ + מרחק של 50 ס״מ לפחות מאביזר מתכתי אחר (מעקה זכוכית מחוסמת בין המרכיבים).

6.5.1.2.3 מינימום שטח רצפה לשער שיקוף אדם (עתידי) 150X150 ס״מ

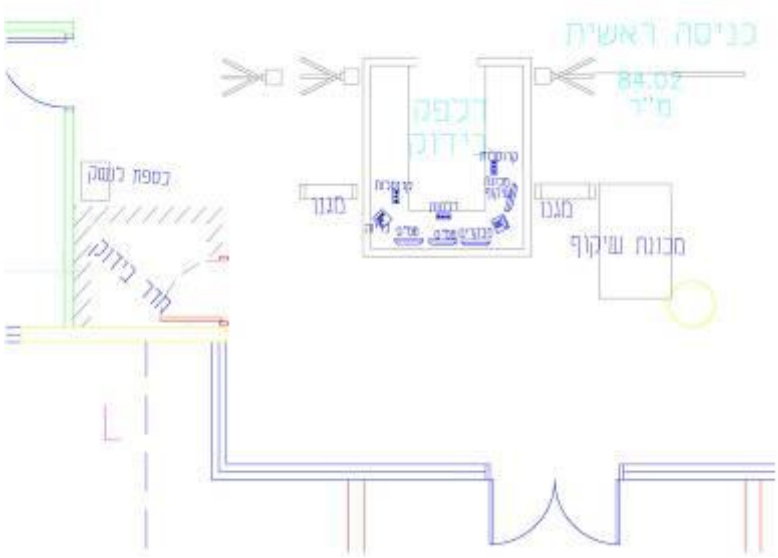
6.5.1.2.4 בתכנון קונסטרוקטיבי של לובי הכניסה יילקח בחשבון משקל ציוד הבידוק שיכול להגיע לעד 1500 ק״ג והצורך בהזנות חשמל ומתח נמוך מאוד.

6.5.1.3 יש לקחת בחשבון כי למתקן עתידים להיות שתי כניסות מבוקרות ראשיות.

6.5.1.4 הכניסה למבנה תיעשה דרך קרוסלות נמוכות מופעלות ע״י בקרת כניסה, וממוקמות באופן שלא תתאפשר כניסה מבלי לעבור דרכן. בחלק מהמקרים יתוכננו קרוסלות בגובה מלא, קרוסלות זכוכית או שערים נפתחים לפי הצורך והתכנון הספציפי.

6.5.1.5 בכל מערך כניסה ראשי תתוכנן עמדת ביטחון בכניסה שתפקח על הבידוק ותפעול מערך הכניסה. גודל העמדה, מיקומה והציוד שבה יתוכנן בהתאם לצרכים הספציפיים.

6.5.1.6 ההצבה המועדפת הינה דלפק מרכזי עם שני נתיבי כניסה משני הצדדים (ראה סקיצה).



סקיצה 1 : מבנה עקרוני של אזור בידוק במערך כניסת הולכי רגל

6.5.1.7 בלובי הכניסה ולפני מערך הבידוק יתוכנן חדרון קטן לבידוק גופני. מומלץ כי החדרון יכלול דלת ננעלת מבפנים ווילון פנימי. שטחו המינימאלי יהיה 1.5X2 מ׳.

6.5.1.8 מומלץ כי דלתות הכניסה והלובי המתואר לעיל יתוכננו תוך לקיחה בחשבון מבנה יעיל מבחינה אנרגטית של מיזוג האויר בהנחה שבאזור הסמוך לדלתות ישהו אנשים. לכן יש לתכנן מערך דלתות אשר ישמור על השפעה מינימאלית של הטמפרטורה בחוץ על הלובי.

6.5.1.9 במבנה מקבל קהל רב מומלץ לתכנן אזור המתנה שיאפשר המתנה למבקרים בזמן שהם ממתינים לאישור כניסה. תכנון השטח הנדרש והריהוט, בהתאם לכמות ואופי המבקרים הצפויים.

6.5.1.10 בכניסה, לפני קו הבידוק, תמוקם כספת / ארוניות לאחסון עצמי של כלי או נשק. מפרט לכספת זו בהתאם להנחיות משטרת ישראל

שמשתנה מפעם לפעם.

6.5.1.11 מומלץ כי נתיבי היציאה מהבניין יהיו בסמוך לאזור כניסת הקהל באופן אשר יאפשר בקרת המאבטחים ויחסוך עלויות ביצוע ותפעול.

6.5.1.12 בכניסות המבקרים בלוביים הראשים ובכניסות לחניונים יהיה שימוש במערכת לזיהוי מבקרים תוך כדי תנועה העושה שימוש בטכנולוגיה של זיהוי פנים, תנועה, קול וכדומה.

6.6 דלתות מוגנות חוץ ופנים:

6.6.1 פירוט:

6.6.1.1 דרישות כלליות מיצרן וקבלן התקנת הדלתות מוגנות:

6.6.1.1.1 על היצרן וקבלן הדלתות להיות יצרן / קבלן מאושר לייצור והתקנת דלתות בהתאם להנחיות מכון התקנים הישראלי, משטרת ישראל, פקע"ר וגופי הביטחון ומוסמך גם לייצור והתקנת דלתות מוגנות לאיום הספציפי (פריצה, הדף, ירי וכד').במידה ונידרש מיגון משולב גם כנגד אש בנוסף לאיומים הפיזיים יוכיח היצרן / קבלן אישורים לעמידות משולב בהתאם לדרישות מכון התקנים הישראלי או מקביל לו.

6.6.1.1.2 על הקבלן להיות קבלן רשום ומוכר כולל במתן שירות קבוע ותחזוקה ללקוחות מוסדיים לפחות בחמש השנים האחרונות. על המוצרים כולם לענות לדרישות התקן הרלוונטי של מת"י פקע"ר ומשטרת ישראל.

6.6.1.1.3 באם לא הגדר אחרת במפורש תכלול דלת גם צילינדר סטנדרטי (שעומד בתקנים הרלוונטיים: ת"י 101,950,21) ותענה לדרישות גורמי הביטחון מנעולי מסטר וכדומה.

6.6.1.1.4 יועץ המיגון של הפרויקט יגיש לאישור סגן ר' מערך סייבר חירום וביטחון במשרד האוצר את פרטי הדלתות.

6.6.1.1.5 כעיקרון יותקנו הדלתות השונות במבנה בהתאם למיפוי שייעשה ע"י הקב"טים הרלוונטיים לעניין האיומים השונים בהם צריכות לעמוד הדלתות ברחבי הבניין ואישור בכתב של הגורמים הרלוונטיים על גבי תוכנית האבטחה של יועץ המיגון.

6.6.1.2 דלת מוגת הדף - תדרש במקומות הבאים:

6.6.1.2.1 דלתות בקיר חיצוני שנותח על ידי היועץ ונמצא שמחייב מיגון כנגד הדף, הדלת תמוגן לרמה שנדרשת ע"י ניתוח הסיכונים שבוצע ע"י יועץ המיגון.

6.6.1.2.2 כל דלת בחדרים מוגנים בהתאם לדרישות פקע"ר (ממ"ד,

ממ״ק, ממ״מ).

6.6.1.2.3 כל דלת בחדרי מצב, בקרה, מחשבים וכד׳ שמתוכננים להיות מאוישים בחירום בהתאם לתוכנית האבטחה שאושרה ע״י הקב״טים של המשרדים המאיישים את המבנה.

6.6.1.2.4 הדלת תהיה מיוצרת ע״י קבלן דלתות בתחום המיגון ואישור פקע״ר לייצור דלתות הדף ותחזוקתן.

6.6.1.3 דלת מוגנת ירי - עשויה להדרש במקומות הבאים :

6.6.1.3.1 במקרה הגדרה ספציפית ע״י הקב״ט המנחה או יועץ המיגון כדוגמה בלשכת שר או אזורים מיוחדים אחרים. רמה מיגון והאיום נגדו נדרשת הדלת לעמוד יוגדר ע״י הקב״ט המנחה מראש ותיושם גם בנוגע לקיר בה מותקנת הדלת.

6.6.1.3.2 הדלת תהיה מיוצרת ע״י קבלן המוכר בתחום דלתות המיגון ומאושר לייצור דלתות ע״י מכון התקנים, בעל דלתות מאושרות לתקן בליסטיקה אירופי EN BR6 או שווה ערך.

6.6.1.3.3 רמת מיגון נגד ירי זהה תהיה לכל חלקי הדלת כולל משקוף והקיר עליו מותקנת הדלת.

6.6.1.4 דלתות מוגנות פריצה אלימה- עשויה להדרש לצרכים הבאים :

6.6.1.4.1 סגירת פתחים בהיקף המבנה כנגד פריצה פנימה לצרכים פליליים, ונדליזם טרור וכד׳ מיגון ואטימת אזורים הדורשים מיגון בטחוני כגון כספות, ארכיונים מסווגים.

6.6.1.4.2 סגירת חדרים ואזורים ממודרים ביטחונית כגון חדרים סודיים, לשכת שר, חדרי מחשב.

6.6.1.4.3 בקרת כניסה לאזורים ממודרים בגלל צנעת הפרט או אחרת כגון : לובי קומתי דלתות כניסה למשרדים , ארכיון פרטי וכד׳.

6.6.1.5 לצורך מיגון וסגירת דלתות בהיקף המבנה כנגד פריצה פנימה יעשה שימוש בדלת מוגנת כנגד פריצה אלימה לזמן עצירה אופטימלי שווה ערך ל 15 דקות. הדלת תהיה מאושרות לתקן פריצה אלימה ברמה הנדרשת ע״י מת״י או אמריקני או אירופי או תקן שווה ערך מאושר אחר :

6.6.1.5.1 European standard ENV 1630:1999 Level 4

6.6.1.5.2 US department of state 12-FAH-5 for 15 minutes resistant.

6.6.1.6 לצורך למיגון אזורים ביטחוניים (כספות, ארכיונים) כנגד פריצה פנימה יעשה שימוש בדלת מוגנת כנגד פריצה אלימה לזמן עצירה אופטימלי שווה ערך ל 5 דקות. הדלת תהיה מאושרות לתקן פריצה אלימה ברמה הנדרשת ע״י מת״י או אמריקני או אירופי או תקן שווה ערך מאושר אחר :

6.6.1.6.1 European standard ENV 1630:1999 Level 3

6.6.1.6.2 US department of state 12-FAH-5 for 5 minutes resistant

6.6.1.7 לצורך למיגון אזורים ממודרים ביטחונית (חדר סודי, לשכת שר, חדר מחשב) כנגד פריצה פנימה יעשה שימוש בדלת מוגנת כנגד פריצה אלימה ברמה הבסיסית דלת פלדה רב בריחית (שווה ערך "רב בריח"). הדלת תהיה מאושרות לתקן פריצה אלימה ברמה הנדרשת ע"י מת"י או אמריקני או אירופי או תקן שווה ערך מאושר אחר :

6.6.1.7.1 European standard ENV 1630:1999 Level 2

6.6.1.8 בבקרת כניסה לאזורים ממודרים (לובי קומה, ארכיון פרטי) כנגד כניסה לא מאושרת יעשה שימוש בדלת מבוקרת ע"י בקרת כניסה וללא התייחסות לעמידותה של הדלת בפני פריצה אלימה, דלתות כניסה למשרדים יעמדו כנגד פריצה אלימה של 2-5 דקות לפחות.

6.6.1.9 עקרונות מנחים לדלתות מוגנות כנגד פריצה אלימה הממוקמות בנתיב יציאות חירום ו/או משמשות גם כדלתות אש :

6.6.1.9.1 דלת ליציאת חירום בלבד תהיה דלת פלדה, תפתח כלפי חוץ, מערכת הצירים תהיה פנימית או מוגנת באופן שיקטין אפשרות לחבלה או חסימת הדלת מבחוץ. ומחזיר השמן יהיה תמיד פנימי. הדלת ללא חור צילינדר חיצוני, במידת הצורך ניתן להתקין מערכת אינטרקום ובקרת כניסה שתאפשר פתיחת הדלת מחדר הבקרה הביטחוני או ע"י כרטיס בקרה מתאים. ניתן ומומלץ בדלתות חירום להשתמש במנעול נעילה מכני או אלקטרו מכאני הנעול תמידית.

6.6.1.9.2 הדלת תהיה מאושרת ע"י מת"י כדלת אש (או מילוט) כולל כל רכיבי המיגון ואבטחה, המשקופים וכד' בהתאם לנדרש תוכנית האבטחה.

6.6.1.10 דלתות למיגון משולב :

6.6.1.10.1 במידה ומערכת השיקולים ובחינת האיומים תדרוש דלת אשר ממלאה גם דרישות פריצה אלימה וגם עמידות בפני הדף ו/או ירי וגם עמידות באש, הכללים האמורים לעיל יצטרפו אלו לאלו ועל הדלת לעמוד בקריטריונים של כל אחד מהנושאים האמורים לעיל.

6.6.1.10.2 בכל מקום בו נדרש הפתח לצרכי מילוט או צורך תפקודי אחר יציע הקבלן פתרון שישלב באופן מלא בין דרישות המיגון לדרישות המילוט לפי ת"י 1212 .

6.6.1.10.3 על תכנון הדלת להתייחס גם למערכות האבטחה הנדרשות לדלת ולוודא התקנה בהתאם לתקני הבטיחות. במידה והדלת הינה דלת מילוט יש לוודא בתקני בטיחות ואש רלוונטיים .

6.7 חלונות, קירות מסך וויטרינות זכוכית מוגנות:

6.7.1 פירוט:

6.7.1.1 ככלל, רמת זיגוג מינימאלית לחלונות בבניין תהיה , זכוכית שכבתית עם שכבה פנימית של PVB בעובי של 1.52 מ״מ.

6.7.1.2 דרישות כלליות מיצרן וקבלן המערכות המוגנות :

6.7.1.2.1 על היצרן וקבלן להיות יצרן / קבלן מאושר לייצור והתקנת המערכות בהתאם להנחיות מכון התקנים הישראלי, משטרת ישראל פקע״ר וגופי הביטחון הרלוונטיים ומוסמך גם לייצור והתקנת המערכות המוגנות לאיום הספציפי (פריצה, הדף, ירי וכד׳). במידה ונדרשת התייחסות משולבת גם לעמידות כנגד אש או אפשרות מילוט יוכיח היצרן / קבלן אישורים לעמידות משולבת בהתאם לדרישות מכון התקנים הישראלי או מקביל לו.

6.7.1.2.2 על הקבלן להיות קבלן רשום ומוכר כולל במתן שירות קבוע ותחזוקה ללקוחות מוסדיים לפחות בחמש השנים האחרונות. על המוצרים כולם לענות לדרישות התקן הרלוונטי של מת״י פקע״ר ומשטרת ישראל.

6.7.1.2.3 יועץ המיגון של הפרויקט יגיש לאישור סגן ר׳ מערך סייבר חירום וביטחון במשרד האוצר את פרטי מערכות המיגון.

6.7.1.2.4 בעיקרון יקבלו כל החלונות, קירות המסך והוויטרינות בבנין התייחסות בתוכנית האבטחה של יועץ המיגון תוך התייחסות לעמידות כנגד הדף, פריצה אלימה ובמקרה הצורך גם ירי. ההתייחסות בתוכנית האבטחה תהיה על רקע ניתוח הסיכונים שתבוצע ובכל מקרה תובא לאישור סגן ר׳ מערך סייבר חירום וביטחון במשרד האוצר לפני העברה לתכנון וביצוע.

6.7.1.3 חלונות, קירות מסך וויטרינות מוגני הדף :

6.7.1.3.1 יידרשו בהיקף המבנה כולו ובעיקר בחזיתות הפונים לכביש או חניון ציבורי. רמת המיגון תקבע בהתאם לניתוח הסיכונים שתבוצע ע״י יועץ המיגון עבור רכב תופת ותוצג לאישור סגן ר׳ מערך סייבר חירום וביטחון במשרד האוצר.

6.7.1.3.2 רמת מיגון כנגד הדף גבוה (מעל 100 psi m sec & 10 psi) תקבע בד״כ למערכות הפונות לכביש ציבורי.

6.7.1.3.3 רמת מיגון כנגד הדף בינוני (מתחת ל 99 psi m & 29 psi Sec) תקבע בד״כ למערכות חיצוניות – נמוכות, שאינם פונים לכביש ציבורי.

6.7.1.3.4 רמת מיגון בסיסית (עד 4 psi & 28 psi m sec) תקבע בדרך כלל למערכות גבוהות או שאינן פונות לאזורים ציבוריים.

6.7.1.4 חלונות, קירות מסך וויטרינות מוגנת ירי :

6.7.1.4.1 עשויה להידרש במקרה הגדרה ספציפית ע"י הקב"ט המנחה או יועץ המיגון כדוגמה בלשכת שר, חדר מחשב, דלפקי קבלת קהל או אזורים מיוחדים אחרים. רמה מיגון והאיום נגדו תידרש המערכת לעמוד יוגדר ע"י הקב"ט המנחה מראש ותיושם גם בנוגע למעטפת, משקופים והקיר בה מותקנת מערכת החלון / קיר מסך / וויטרינה.

6.7.1.4.2 מערכת החלון תהיה מיוצרת ע"י קבלן המוכר בתחום החלונות המוגנים ומאושר לייצור חלונות (רגילים) ע"י מכון התקנים, בעל חלונות מאושרות לתקן : בליסטיקה אירופאי EN BR6 או שווה ערך.

6.7.1.5 חלונות , קירות מסך וויטרינות מוגנות פריצה אלימה :

6.7.1.5.1 תידרש לסגירת פתחים בהיקף המבנה כנגד פריצה פנימה לצרכים פליליים, ונדליזם טרור וכד' כולל בנוסף מקרים מסויימים במרפסות חיצוניות באזורים מיוחדים כגון משרד שר וכד' בהתאם להחלטת יועץ המיגון של הפרויקט ואישור סופי של סגן ר' מערך סייבר חירום וביטחון במשרד האוצר.

6.7.1.5.2 לצורך מיגון וסגירת חלונות, קירות מסך זכוכית וויטרינות בהיקף המבנה כנגד פריצה פנימה יעשה שימוש בדלת מוגנת כנגד פריצה אלימה לזמן עצירה אופטימלי שווה ערך ל 15 דקות. מערכת המיגון תהיה מאושרות לתקן פריצה אלימה ברמה הנדרשת ע"י מת"י או אמריקני או אירופי או תקן שווה ערך מאושר אחר :

European standard ENV 1630:1999 Level 4
US department of state 12-FAH-5 for 15 minutes resistant

6.7.1.6 חלונות, וויטרינות וקירות מסך זכוכית למיגון משולב :

6.7.1.6.1 במידה ומערכת השיקולים ובחינת האיומים תדרוש מערכת מיגון שמלאה גם דרישות פריצה אלימה וגם דרישות מיגון או בטיחות נוספות תתוכנן המערכת תוך התייחסות לכל מכלול ההנחיות יחד.

6.7.1.6.2 ככלל במידה ויאופיינו חלונות לפתיחה הפתיחה תהיה קיפ חיצוני עליון .

6.8 הנחיות תכנון אמצעים באזורים מוגנים בתוך המבנה

6.8.1 כספת נשק מרכזית –

6.8.1.1 חדר נשק יבנה בהתאם להנחיות משטרת ישראל בהתאם להנחיות הרלוונטיות שמתעדכנות מפעם לפעם באתר חטיבת האבטחה באתר משטרת ישראל באינטרנט.

6.8.1.2 בעקרון יאוכסנו מעל 21 כלי נשק בחדר שהוגדר כ"חדר נשק", נבנה עם קירות בטון מזוין היקפי בעובי 20 ס"מ לפחות (כולל תקרה ורצפה), איננו כולל חלון וסגור באמצעות דלת "כספת" מיוחד שאופיינה כדלת חדר נשק.

6.8.1.3 חדר זה ייבנה עפ"י מפרט 90.91 ו 90.92 כולל מערכת אזעקה עפ"י תקן 90.96 של משטרת ישראל ותקן 1337 של מת"י.

6.8.1.4 בכניסה לחדר תותקן מערכת בקרת כניסה.

6.8.2 ארון/ כספת נשק למאבטחים

6.8.2.1 עפ"י הנחיות המשטרה נדרשים כלל המאבטחים להפקיד את נשקם בתוך חדר הנשק המצויין לעיל.

6.8.2.2 לאור כך נדרש היזם להתקין כספות מאושרות להפקדת נשקים ע"י משטרת ישראל בתוך חדר הנשק המרכז.

6.8.2.3 מספר הכספות בהתאם למספר המאבטחים הצפויים לאבטח את המתקן.

6.8.2.4 הכספת תעמוד באופן מלא במפרט 90 של משטרת ישראל לכספת לאחסון נשקים

6.8.2.5 יש לשים לב לנושא העמסת משקל על הרצפה בהקשר זה

6.8.3 כספת אחסון נשקים אישיים של מבקרים –

6.8.3.1 בהתאם להנחיות משטרת ישראל יש צורך במיקום כספת להפקדת נשק אישי בכניסה לכל מבנה ציבור מקבל קהל.

6.8.3.2 כספת כנ"ל תמוקם בלובי הכניסה הראשי, לפני אזור הבידוק ותוך הקפדה כי אזור ההפקדה יהיה בקרבת עמדת המאבטח ובקו ראיה ישיר איתו.

6.8.3.3 אפיון הכספת ואישורה יעשה בהתאם להנחיות משטרת ישראל בהתאם להנחיות הרלוונטיות שמתעדכנות מפעם לפעם באתר חטיבת האבטחה באתר משטרת ישראל באינטרנט ובאישור סגן ר' מערך סייבר חירום וביטחון במשרד האוצר.

6.8.3.4 על הספק לעסוק בתחום זה של ייצור כספות – כולל "תאים לאחסנת

נשק״, ומתן שירות קבוע ללקוחות מוסדיים בחמש השנים האחרונות לפחות. המוצרים יענו לדרישות התקן הרלוונטי של מת״י, ומשטרת ישראל (מפרט 90.91).

6.8.3.5 תותקן מצלמה הצופה על הכספת

6.8.3.6 הכספת תוצב בתוך ארונית .

6.8.3.7 על המידות וכמות התאים יוחלט יחד עם קב״ט המתקן .

6.8.4 ארכיון / כספת לאחסון מזומנים או חומר סודי –

6.8.4.1 בהתאם לצורך ודרישות הקב״טים המאכלסים והנחיות סגן ר׳ מערך סייבר חירום וביטחון במשרד האוצר ימוקמו כספות לאכסון חומר סודי, נשק, כספים או כל ציוד אחר בקומות המבנה השונות.

6.8.4.2 בעקרון יהיו חדר הכספות בנויות בבניה מסיבית – קיר בטון מזוין בעובי 10-15 ס״מ או לבנים מלאות או שווה ערך מאושר, ללא חלון כלל ועם דלת עמידה בפריצה אלימה למשך 5 דקות לפחות. מומלץ למקם חדרים אלו בגרעיני מבנה.

6.8.4.3 יש לקחת בחשבון כי בחדר הכספות ימוקמו בדרך כלל כספות או מדפים כבדים ולכן יש לתכנן את העומס השימושי על הרצפה בלפחות 300 ק״ג.

6.8.5 כספות פלדה –

6.8.5.1 כספות פלדה לאחסון כסף, חומרים סודיים או עד 20 כלי נשק, ימוקמו בעקרון בתוך חדר ארכיון / כספת.

6.8.5.2 אפיון הכספת עצמה יבוצע בהתאם להנחיות הגוף המנחה ואינן באחריות יועץ המיגון של הפרויקט. בתכנון החדר יש לקחת בחשבון את משקל הכספות שיכול להגיע לעד 500 ק״ג למ״ר.

6.8.5.3 מיגון הכספות באמצעים אלקטרוניים בהתאם להנחיות ס׳ראש מערך סייבר חירום וביטחון ובהתאם להנחיות הגופים המנחים.

6.9 חדרים ואזורים מוגנים

6.9.1 פירוט:

6.9.1.1 מתחם מחלקת אבטחה : בקומת הקרקע או בסמיכות ישירה יתוכנן אזור ביטחון שיכלול :חדר קב״ט (15 מ״ר, חדר ס.קב״ט (10 מ״ר), מזכירות (10 מ״ר), חדר בקרה (40 מ״ר)- חדר הבקרה ימוקם במתחם המוגן ביותר במבנה עמידות מתחם זה לא תפחת מעמידות

המקסימלית הניתנת ליחידות המאכלסות את המתקן בחירום(חדרי המצב) , חדר ציוד לתקשורת (10 מ״ר), מחסן נשק (15 מ״ר), מחסן ביטחון לציוד (10מ״ר), חדר מאבטחים/מנוחה (25 מ״ר), שירותים (7 מ״ר), מטבחון (5מ״ר). המתחם ימוקם בקרבה מיידית לאזור הכניסות תוך נגישות מהירה ללובי הכניסה המרכזי, היציאות מהמבנה וגם חדרי המעליות המרכזיים. המתחם יהיה ממודר וסגור לכניסת עובדים שאינם מורשים.

6.9.1.2 חדר בקרה ביטחוני – חדר הבקרה הביטחוני יבנה כחדר מצב בטחוני באפיון טכני זהה לאפיון ממ״ק כולל מערכת סינון אב״כ מקומית עבור חדר זה + חדר הציוד הטכני שלו- לפחות. על היזם לקחת בחשבון כי ייתכן ואיום היחוס המעודכן ידרוש אפיון טכני מחמיר מזה של ממ״ק. דלת הכניסה אל חדר הבקרה תהיה דלת ממ״ק תקנית ודלת נוספת לצורכי תפעול שוטף – עליה יותקנו מערכות בקרת הכניסה הכניסה למתחם הביטחון תהיה באמצעות תא סינון מבוקר הדלת החיצונית לתא הסינון תעמוד בפריצה אלימה ל - 15 דקות לפחות.

6.9.1.3 חדר משרדי המסווג ברמת סודי ומעלה – חדר שיוגדר כחדר משרדי רגיל אשר משמש לעובדים עם חומר סודי ו/או שמאוחסן בו לצורכי עבודה חומר סודי (בשונה מארכיון או חדר כספות) יבנה עם קירות, דלתות וחלונות עמידים בפריצה אלימה לרמה של 5 דקות (ראה במפרט לעיל) תכנון עקרוני ובקשות ל״שווה ערך״ יוגשו לקב״ט הרלוונטי בשלבי התכנון הראשוני.

6.9.1.4 חדר מצב ביטחוני – בהתאם לדרישות הדיור הממשלתי ו/או הקב״טים יתוכננו חדרי מצב ביטחוניים בקומות הבניין. החדרים ימוקמו בשאיפה בקומות המרתף או בגרעיני מבנה במטרה לאפשר גישה בטוחה בזמן חירום ושרידות במקרה פגיעה ישירה בבניין. החדרים יתוכננו ויבנו בדיוק בהתאם לאפיונים והדרישות הטכניות של פקע״ר לחדרי מצב ויכללו גם מערכות טיהור אב״כ אקטיביים. בחדרים אלו יונחו תשתיות מוגברות של מערכות תקשורת ואנרגיה מגובה UPS וגנראטורים.

6.9.1.5 בנוסף לדרישות המשרדים עפ״י הסעיף לעיל , יש לתכנן חדר מצב עבור יחידת הביטחון בגודל 30 מ׳ על מנת לאפשר שרידות גם במצבי חירום של כלל מערכות האבטחה.

6.9.1.6 חדר התקשרות של מערכות האבטחה נדרש להיות בצמוד לחדר זה.

6.9.1.7 חדרי מחשב – חדרי מחשב באשר הם יקבלו תשומות מיגון ואבטחה בהתאם להנחיות קב״ט ואחראי מערכות המידע. במידת הצורך ימוגן חדר המחשב ברמה של חדר מצב בטחוני לעיל (בדרך כלל מחשב מרכזי ו/או המשמש את המשרד לצורך פעילות בשעות חירום ומלחמה). כרמת מינימום ביטחוני יבנה חדר מחשב כאזור ממודר באופן מלא כולל קירות היקפיים וחלונות מוגנים כנגד פריצה אלימה לרמה של 5 דקות כמפורט לעיל.

6.10 חניון פנימי ואזור פריקת /. טעינת סחורות

6.10.1 חניון ציבורי או משולב-

6.10.1.1 בכל מצב של חניון משולב המשמש גם כחניון ציבורי יתוכנן מרחב בדיקה בכניסה לחניון כולל גם אפשרות סירוב וסיבוב הרכב הנבדק לאחור מבלי להיכנס לחניון. על יועץ המיגון להבטיח כי פיצוץ רכב תופת במשקל הקריטריון לא תפגע ביציבות המבנה ותגרום לנזק "נסבל" בלבד.

6.10.1.2 כל חדרי המדרגות והמעליות מהחניון הציבור יסתיימו מחוץ למבנה או לפחות מחוץ לאזור המאובטח במבנה. כניסה למבנה תתאפשר רק דרך לובי הבידוק המרכזי

6.10.1.3 על יועץ המיגון להבטיח כי קומות החניון יתוכננו ויבנו באופן שפיצוץ מטען קטן (עד 20 ק"ג ט.נ.ט) לא יגרמו לנזק בקומות הכניסה ו/או המשרדים.

6.10.1.4 ההגנה מפני אש תתוכנן בכל מקרה כך שהחניונים יהיו מנותקים לחלוטין ממבנה המשרדים (גם הנחיות הבטיחות מחייבים זאת).

6.10.2 חניון פרטי-

6.10.2.1 במידה ומתוכנן חניון פרטי לשימוש משרדי הממשלה בלבד והכניסה אליו מבוקרת ונשלטת ע"י בקרת כניסה ו/או מאבטחים, ניתן לתכנן עליות ישירות מהחניונים אל קומות המשרדים תוך מעבר דרך קרוסלות בקרת כניסה בגובה מלא שמאפשרת כניסת אדם אחד בלבד בכל סיבוב וכל שאר הכניסות חסומות ומבוקרות. לחילופין יש לנקוט בגישת כניסה כבחניון ציבורי (יציאה לשטחים ציבוריים לפני אזור הבידוק), הכל בכפוף לאישור התכנון על ידי ס. ראש מערך סייבר חירום וביטחון במשרד האוצר לפתרון המוצע.

6.10.3 אזור פריקה וטעינת סחורות-

6.10.3.1 בשאיפה ימוקם אזור הפריקה והטעינה מחוץ למבנה ו/או רחוק עד כמה שניתן מגרעין המבנה ובכל מקרה מחוץ לאזור המשרדים הראשי.

6.10.3.2 אזור הפריקה רצוי שיהיה פתוח לאוויר החופשי (לא בחלל סגור), ובמרחק רב עד כמה שניתן מעמודי מבנה ראשיים, במרחק מינימאלי של 10 מטרים. על יועץ המיגון להראות כי אירוע פיצוץ / שרפה משמעותי באזור זה לא יגרום לנזקים משמעותיים למבנה וליושבים בו בהתאם לאיום הייחוס הרלוונטי למתקן שיימסר ליועצי המיגון המאושרים לפרוייקט.

6.11 מפתחות וצילינדרים

6.11.1 מערכת מאסטר-

6.11.1.1 כל הצילינדרים בבניין יהיו חלק ממערכת מאסטר אחידה בתכנון היררכי /מטריציוני.

6.11.1.2 מערכת המאסטר תהיה מתוצרת מולטילוק רב בריח או שווה ערך עם חלוקה לרמות בהתאם לצרכי המשרדים עפ״י הגדרות הקב״ט אך לא פחות מ שש רמות.

6.11.1.3 הגדרת הרמות השונות של המערכת ייעשו בתיאום עם סגן ר׳ מערך סייבר חירום וביטחון במשרד האוצר.

6.11.1.4 יובהר כי יסופקו לפחות 5 מפתחות עבור כל צילינדר כמות התפתחות הסופית לפרוייקט תהיה מכפלת הצילינדרים ב חמש , החלוקה בפועל תהיה בהתאם לצרכי המשרדים והגדרות הקב״ט .

6.11.1.5 התקנת מערכת המאסטר תעשה לאחר מסירת המתקן למזמין ולפני אכלוס המתקן על ידי המשרדים, יודגש כי פרק זמן זה הינו פרק זמן קצר מאוד ועל קבלן הצילינדרים לבצע את ההתקנה בהתאם ללוחות הזמנים וסדרי עדיפויות שיוגדרו על ידי קב״ט המתקן.

6.11.1.6 מסירת המערכת והמפתחות – הקבלן מתחייב למסור בכל יום עבודה את הצילינדרים והמפתחות שהותקנו באותו יום לקב״ט המתקן בצורה מסודרת ויעילה עפ״י נוהל עבודה שייקבע בין הקב״ט לחברה המתקינה.

6.11.1.7 הספק מתחייב לספק למתקן את מערכת הצילינדרים והמפתחות בטכנולוגיה המתקדמת ביותר הקיימת במעמד ההתקנה .

6.11.1.8 הספק יעניק אחריות של שנתיים על הצילינדרים ומתחייב להחליף כל צילינדר שאינו תקין בצילינדר חדש.

6.11.1.9 לפחות 30% מהצילינדרים שיותקנו בדלתות המבנה יעמדו בתקן skg הולנדי אירופאי לצילינדרים מיקום התקנת צילינדרים אלו ייקבי על ידי קב״ט המתקן.

6.11.1.10 מערכת הצילינדרים והמפתחות שיסופקו יהיו מסומנים על גוף הצילינדר ועל המפתח.

6.11.1.11 ספק המערכת יספק מכונת שכפול מפתחות וכן גלמים ייחודיים המוגדרים עבור מבני ממשלה וממסד (שאינם מסופקים במגזר הפרטי) כמות הגלמים שיסופקו יעמוד על 500. הקבלן מתחייב כי יוכל להמשיך ולספק גלמים אלו במהלך עשור לפחות ממועד ההתקנה.

6.11.1.12 הספק יכשיר איש אבטחה/תחזוקה לטיפול בצילינדרים תקולים וכן בביצוע תיקון והחלפת צילינדרים במתקן וכן יכשיר אותו לשימוש במכונת השכפול לפחות אחת לשנה.

מתח נמוך- דגשים מיוחדים ואפיון טכני

6.12 כללי

6.12.1.1 מכיוון שמערכת הביטחון ומערכות בקרת המבנה מוגדרות כמערכת מבוססת IP על המציע לקחת בחשבון כי כלל מערכות הביטחון ובקרת המבנה לרבות ארונות התקשרות יהיו מוגנים בטכנולוגיה נגד תקיפת סייבר. תפקיד של מערכת זו לנתר, להתריע ולמנוע תקיפות סייבר על המערכת. דוגמת מערכת SYBER SWITCH או פתרון אחר שווה ערך שיאושר ע"י המזמין.

6.12.1.2 בנוסף, על המציע לקחת בחשבון התקנת מערכת back-bone שאמורה לגבות את כלל המערכת.

6.12.1.3 קיים איסור על התחברות מרחוק והתחברות לאינטרנט של מערכת המנ"מ ומערכות בקרת המבנה חיבור מרחוק לכל מערכת אלקטרו מכאנית אחרת מחוייב באישור מקדים של קב"ט המתחם .

6.12.1.4 כלל עדכוני התוכנה יבוצעו על ידי מחשב נייד ייעודי ומוקשח ולא מחובר לאינטרנט.

6.12.1.5 בכל חצי שנה לפחות מתחייב ספק המערכות לבצע עדכון תוכנה .

6.12.1.6 כלל עדכוני מערכת ההפעלה /תוכנה יבוצעו דרך מערכת הלבנה מאושרת על ידי מערך הסייבר של המשרד.

6.13 מערך תקשורת TCP\IP ייעודי לביטחון

6.13.1 תשתיות מחשוב

6.13.1.1 תוקם במסגרת פרוייקט זה רשת תקשורת אחודה לביטחון שתהיה נפרדת ברמה הפיזית ממערכות התקשורת והטלפוניה השחורה\אדומה. רשת זו תשרת אך ורק את מערכות הביטחון.

6.13.1.2 מערך התקשורת שיוקם ישרת את מערכות הביטחון כולל בין היתר את מערכות הטמ"ס,אינטרקום,פריצה ובקרת כניסה.

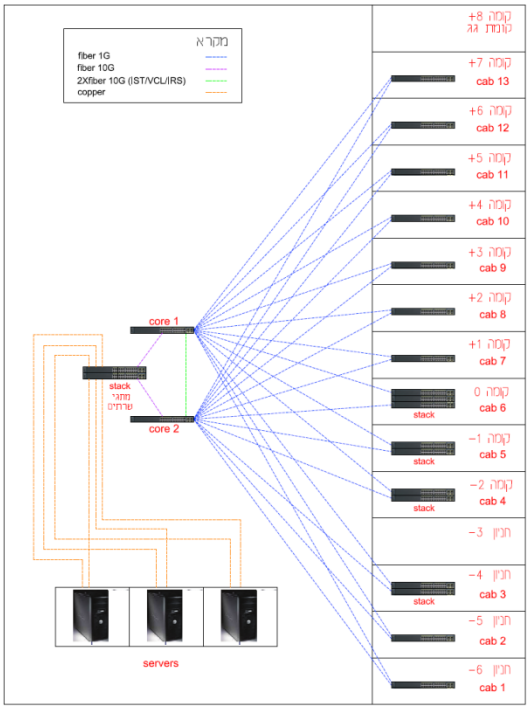
6.13.1.3 תשתית זו תיצור למזמין תשתית אמינה ומתקדמת ותאפשר קישור איכותי של המשתמשים השונים של מערכות הבטחון וברמת שרידות גבוה ביותר שוות ערך לרמת השרידות שהוגדרה למערכות התקשורת בתת הקרקע של המתקן.

6.13.1.4 מערך התקשורת יהיה בצורת\טופולוגיית "כוכב" על מנת ליצור שרידות תוך שימוש בחיבור בין מתגי ה CORE בטכנולוגיית IRF או

VSS של HP או CISCO בהתאמה או טכנולוגיה שוו״ע מאושרת.

6.13.1.5 כל שרת\מחשב יחובר לשני מתגי ה CORE או מתגי השרתים לצורכי שרידות. כמו כן כל מתג קצה יחובר באמצעות שתי סיבים נפרדים למתגי ה CORE ליצירת שרידות מלאה.

6.13.1.6 תרשים טופולוגיית תקשורת עקרוני (כמות הריכוזים והקומות – בהתאם למבנה הבניין) :



6.13.2 עקרונות הטופולוגיה

6.13.2.1 יותקנו לפחות שני מתגי CORE שיחוברו בינם לבין עצמם באמצעות ממשקים G10 בטכנולוגיית VSS\IRF של חברות HP או CISCO בהתאמה או בטכנולוגיה שוו״ע מאושרת.

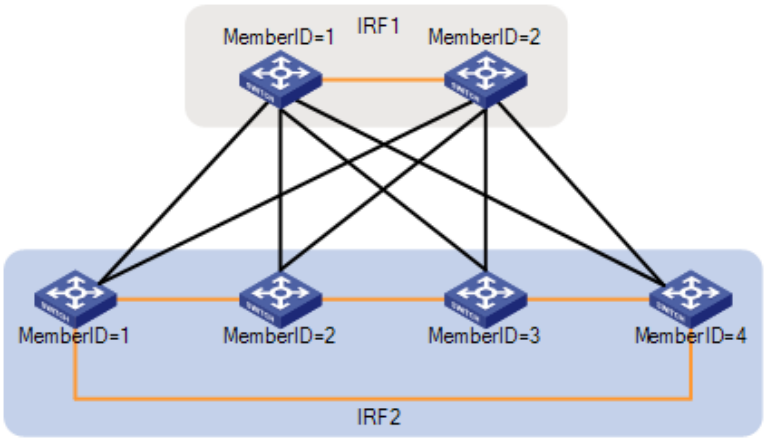
6.13.2.2 כמו כן בכל ריכוז קצה בו יש יותר ממתג אחד – יחוברו המתגים אחד לשני

6.13.2.3 בחיבור VSS\IRF של חברות HP או CISCO.

6.13.2.4 כל מתג קצה יחובר לשני מתגי ה CORE לאיזון עומסים ושרידות.

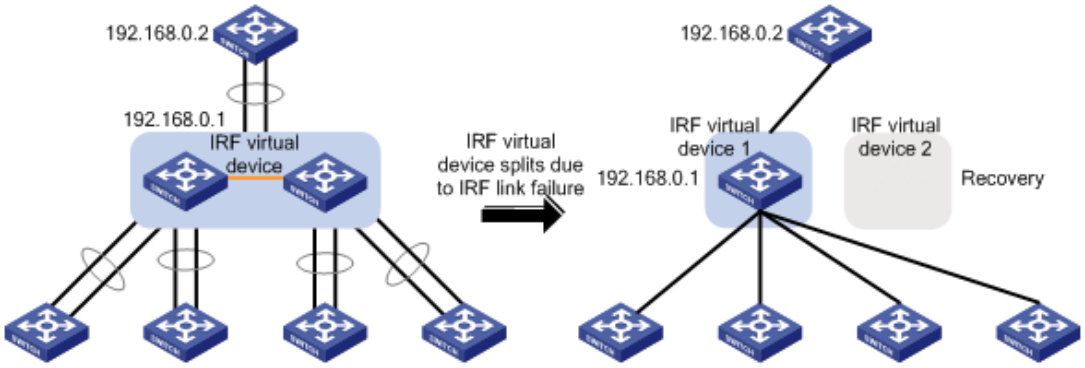
6.13.2.5 להלן תרשים עקרוני להמחשת אופן החיבור (תרשים זה מראה שימוש

בטכנולוגיית IRF של HP לשם המחשה בלבד):



6.13.2.6 אופן חיבור המתגים ותצורת הרשת תאפשר שרידות ברמה גבוה. מתגי ה CORE יפעלו בתצורת ACTIVE-ACTIVE ויאפשרו המשך עבודה גם במצב בו מתג CORE אחד נופל וכן ניתוק אחד מחיבורי הרשת בין ריכוזי הקצה למתגי ה CORE.

6.13.2.7 להלן תרשים עקרוני להמחשת יכולות השרידות הנדרשות (תרשים זה מראה שימוש בטכנולוגיית IRF של HP לשם המחשה בלבד):



6.13.2.8 כל שרתי מערכות הביטחון יחוברו בשני חיבורים רשת GB1 לשני מתגי ה CORE לצרכי שרידות.

6.13.2.9 תסופק שרת מערכת ניהול רשת להגדרת הרשת בקרה ניתור ותפעול

6.13.3 תשתית התקשורת תבוסס על מספר פתרונות נדרשים:

6.13.3.1 תשתית מבוססת כבילת BACK BONE אופטית בין יחידות ה

SWITCH שיותקנו בחדרי התקשורת ובמסדי התקשורת.

6.13.3.2 תשתית נחושת אל אביזרי הקצה ואביזרי קצה.

6.13.3.3 (שקעים/פנלים/מגשרים) מסוככים.

6.13.3.4 נקודות הקצה מהסוגים השונים

6.13.3.5 הציוד האקטיבי ופאסיבי להפעלת רשת הביטחון.

6.13.3.6 באופן עקרוני, בכל נקודה נדרשת יותקן שקע תקשורת RJ-45.

6.13.3.7 תכנון מפורט

6.13.3.8 באחריות היזם לבצע תכנון מפורט המתבסס על דרישות פרק זה בכל ההיבטים הנדרשים להבטחת עמידה בדרישות השונות במפרט זה, פעילותם התקינה של כלל רכיבי המערכות ושילובם במערך הכולל.

6.13.4 התכנון המפורט יכלול בין השאר היבטים אלה:

6.13.4.1 תכנון מרכיבי המערך השונים ופריסתם באתר בהסתמך על התכנון. הקבלן ראשי להציע שינויים המשפרים ומייעלים את התכנון.

6.13.4.2 תכנון נקודות וציוד הקצה השונים באתר.

6.13.4.3 תכנון חדרי התקשורת הראשיים, המשניים והקישורים ביניהם.

6.13.4.4 תכנון כבילה, חיווט, גישור, סימונים וכו'.

6.13.4.5 אינטגרציה בין רכיבי המערכת.

6.13.4.6 ממשק בין המערכות ורכיביהן למערכות משיקות.

6.13.4.7 כל שאר הציוד והעבודות הנדרשים למימוש מלא ותקין של המערכות.

6.13.4.8 עבודות תשתית והתקנות

6.13.4.9 התחלת עבודת ההתקנות של הקבלן מותנית בקבלת אישור מוקדם מהמזמין, על בסיס אישור התכנון המפורט.

6.13.4.10 עבודת ההתקנה תיעשה על פי דרישות המפרט ובהתאם לתכנון המפורט של ההתקנות, שיעשה הקבלן, לאחר אישורו של המזמין.

6.13.4.11 בכל מקרה, כוללת עבודת ההתקנה הנדרשת את כל פעולות התכנון, יצור, אספקה, העברת כבלים, צנרת, חיווט, התקנת המערכות השונות, בדיקות, הפעלה, הדרכה והטמעה של כל אחד מפרטי הציוד השונים הנדרשים לפעולה תקינה ומלאה של המערכת, בהתאם למפרטים הטכניים הספציפיים, בהתאם לנדרש על פי מפרט זה ובהתאם לנדרש במסמכים רלוונטיים נוספים.

6.14 CCTV טלוויזיה במעגל סגור

6.14.1 פירוט:

6.14.1.1 תסופק ותותקן מערכת טמ״ס בטכנולוגיה מתקדמת כפי שמפורט בהמשך, המערכת תשלוט ותבקר על האזורים הבאים :

6.14.1.1.1 היקף חיצוני של המתקן 360 מעלות.

6.14.1.1.2 כניסות, שערים ומבואות.

6.14.1.1.3 אזורים רגישים בתוך המבנה.

6.14.1.1.4 לובי הכניסה + עמדות הבידוק (מספר זוויות)

6.14.1.1.5 דלתות מבוקרות מרחוק (פנימיות).

6.14.1.1.6 בלובי המעליות בכל קומה במתקן.

6.14.1.1.7 נקודות נוספות עפ״י קביעת הקב״ט.

6.14.1.2 בחדר שליטה ובקרה לביטחון ובמוקדי המשנה תתאפשר צפייה בשוטף של מספר אזורים חיוניים ואפשרות מיתוג ידני או אוטומטי לקבלת תמונות מאזורים אחרים.

6.14.1.3 כל המצלמות והמוניטורים יהיו בצבע ומותאמים לצפייה ביום ובלילה.

6.14.1.4 אופן כיסוי השטח ומיקום המצלמות יקבעו בנפרד ע״ג התכניות האדריכליות, בתאום מלא עם הקב״ט .

6.14.2 תיאור כללי

6.14.2.1 מערכת טלוויזיה במעגל סגור – CCTV תאפשר את ביצוע כל פונקציות הצפייה והשליטה הנדרשות ממוקד הבקרה על מערכות מבוזרות ברחבי המבנה.

6.14.2.2 המערכת הנדרשת תהיה בנויה ממצלמותIP HD ומצלמות FULL HD, מערכת הקלטה וניהול וידיאו מרכזית ברשת מחשבים מסוג NVR . מרכזי הצפייה העיקריים יהיו בשולחן הבקרה הראשי חדר הקב״ט ומקומות נוספים על פי הגדרת המזמינה.

6.14.2.3 מערכת ההקלטה תהיה מבוססת תוכנה בלבד. שרת המערכת ניהול הוידאו וההקלטה יהיה מדגם DELL R720XD או שוו״ע מאושר. כולל נפח אחסון כלל המצלמות באיכות מקסימלית וב 25 פריים לשניה ולמשך 30 יממות. כל שרת ינהל עד כ 40 מצלמות לכל היותר. מערך ההקלטה יעבוד בתצורת N+1 (שרת גיבוי).

6.14.2.4 כל המצלמות המוצעות על ידי הקבלן יהיו מיוצרות באירופה, ארה״ב או יפן בלבד.

6.14.2.5 כל מרכיבי המערכת והמצלמות ויתמכו בהעברת/צפייה/שליטה על מצלמות IP.

6.14.2.6 זיווד המצלמות : כל המצלמות בפרויקט זה יזוודו בזיווד DOME אלא אם צוין אחרת.

6.14.3 **מערכת CCTV הטמ"ס תכלול את המרכיבים הבאים:**

6.14.3.1 מצלמות CCTV קבועות ו- PTZ בטכנולוגית IP POE ו POE+ בעלות חיישנים ברזולוציה HD ו FULLHD ומותאמות לצפייה גבוהה בתנאי תאורה משתנים (יום ולילה).

6.14.3.2 מצלמות שיותקנו באיזורי אור וצל בעיתיים – יאופיינו מצלמות בעלות יכול WDR 130dB לפחות ויכולות תיקון תמונה DSP איכותיות ומוכחות.

6.14.3.3 זיווד המצלמות החיצוניות יהיה מותאם לתנאי OUTDOOR 66 IP.

6.14.3.4 כלל המצלמות והמסכים יעוקרו מכניסות רכיבי זיכרון מיותרים ושאינם בשימוש כדוגמת חריצי כרטיס זכרון או כניסות תקשורת במסכים.

6.14.3.5 פריסת תשתיות על רשת תקשורת TCP/IP

6.14.3.6 המצלמות יוזנו ממתג התקשורת בשיטת POE\+POE.

6.14.3.7 מערכת הקלטה דיגיטאליות ברשת NVR כולל שרתים לשמירת מידע על פי הנחיות מפרט טכני זה.

6.14.3.8 מערכות שו"ב הכוללת חומרה ותוכנה לצפייה, קבלת התראות ואחזור חומר.

6.14.4 **המערכת נדרשת לממשק עם מערכת השו"ב כמפורט להלן. נדרש כי המערכת תאפשר לפחות:**

6.14.4.1 צפייה בווידיאו חי – נדרשת אפשרות צפייה בווידיאו חי בעמדות קליינט של תוכנת השו"ב.

6.14.4.2 החלפה מתוזמנת בין מצלמות בפרקי זמן קבועים (Virtual Tour) – כנ"ל, בתנאי שלא יפגום בתרחישי הפעלה והנהלים בחדר הבקרה.

6.14.4.3 שליפת וידאו שהוקלט במערכת – יכולת אחזור בסיסית של וידאו במערכת.

6.14.4.4 ייצוא תמונה מתוך הווידיאו (Snapshot) – יכולת לשמירה מקומית של תמונה מוקפאת במחשב הקליינט.

6.14.4.5 ניהול מצלמות מתנייעות (כולל שליחה ל – preset שהוגדר במערכת) –

תוך מתן עדיפות מלאה לחדר הבקרה לניהול מערכת הווידיאו וניהוג מצלמות הביטחון.

6.14.4.6 המערכת תתמוך ביכולת ניתוח תוכן לרבות אפשרות קבלת התראות במערכת באמצעות אלגוריתם ה – VMD וכל התראה אחרת . מודול ניתוח תוכן יהיה חלק בלתי נפרד מתוכנת המערכת.

6.14.4.7 יכולת להתחיל ולהפסיק הקלטה - – יכולת לשמירה מקומית של וידאו במחשב הקליינט באמצעות תוכנת השו״ב.

6.14.4.8 יכולות תחקור מתוחכמות ומערכת תיחקור כדוגמת BRIFCAM או שוו״ע מאושר.

6.14.5 מערכת הקלטה דיגיטאלית

6.14.5.1 המערכת תיתן פתרון מלא לניהול, גיבוי, הקלטה, שליטה ,איחזור ואינטגרציה בין כל המרכיבים של מערכת הטמ״ס.

6.14.5.2 המערכת תהיה כדוגמת, DVTEL,MILSTONE,GENETEK או שוו״ע מאושר.

6.14.5.3 המציע יספק מערכת מדף הכוללת את הרכיבים העיקריים כמפורט להלן :

6.14.5.3.1 שרת\י ניהול ומיתוג מסוג DELL R720XD או שוו״ע מאושר כמפורט בהמשך.

6.14.5.3.2 תחנת צפייה שליטה וניהול ראשית למשתמשים.

6.14.5.3.3 תחנות צפייה באתר אצל בעלי תפקיד על רשת TCPIP.

6.14.5.3.4 מתגים ורשת תקשורת נתונים.

6.14.5.4 תוכנת הקלטה וניהול נתוני וידאו דיגיטאליים תתמוך בסביבת Windows 2003 server/XP pro לפחות. התוכנה תאפשר תצפית עצמאית מתחנות מרובות לצד פעולות של הקלטה ואחסון.

6.14.6 ערוץ Video Analitics

6.14.6.1 יש לכלול במערכת ניהול הוידאו ובממשק מלא איתה – מערכת video Analitics למספר ערוצים שיבחרו כערוצי VA. כמות הערוצים הללו לא יעלה על 20.

6.14.6.2 נדרשת מערכת גילוי תנועה בזמן אמת בכל מזג אוויר (למעט מצבי קיצון).

6.14.6.3 יוצע ציוד מתוצרת מוכרת ומוכחת ולאחר קבלת אישור היועץ למעט ציוד המאושר להצעה במכרז ומצוין במסמך זה ,IO IMAGE, AGENT VI, VIDEO IQ.

6.14.6.4 מערכת ניתוח אותות הווידאו תהיה משולבת במערכת הווידאו הכללית.

6.14.6.5 המערכת תהיה מודולארית ותאפשר ביצוע אנליטיקה ע"ג שרת/ים מרכזיים וכן ביחידת הקצה ע"פ דרישה מבצעית ו/או דרישת הלקוח.

6.14.6.6 ניתן יהיה לבצע אנליטיקה למצלמות מסוגים שונים, אנלוגי (בעזרת דוחסים) מצלמות IP ו-HD.

6.14.6.7 יתאפשר שילוב מצלמות PTZ במערכת.

6.14.6.8 במידה והתאורה במקום לא תספיק או תאפשר פעולת מערכת תקינה תסופק תאורת א.א ע"מ לאפשר עבודת מערכת תקינה, על הספק לציין זאת במענה למכרז ולתמחר עלות של פנס א.א בזווית של 60 מעלות למרחק של 60 מטר.

6.14.6.9 נדרשת יכולת זיהוי אדם (התרעה על חדירה) במתאר גדר במרחק נתון של 50 מטר מנקודת הגילוי הראשונה ועד נקודת הגילוי האחרונה, יודגש כי זווית הצפייה של המצלמה בקו גדר לא תפחת מ30 מעלות ולא תעלה על 50 מעלות.

6.15 בקרת כניסה

6.15.1 שער מגנומטר:

6.15.1.1 שער המגנומטר יותקן בכל מעבר כניסת אזרחים ועפ"י תאום מראש מול סגן ר' מערך סייבר חירום וביטחון במשרד האוצר.

6.15.1.2 שערי מגנומטר – המאושרים ע"י הגורמים המנחים (מוטות עגולים כולל אינדיקציה על גובה המתכת עם 16 נוריות) או פנלים שטוחים עפ"י בחירת האדריכל.

6.15.1.3 מכשיר המגנומטר המוצע ע"י החברה יהיה מדגם ומסוג המאושר לשימוש בגופים ממלכתיים ביטחוניים במדינת ישראל עפ"י רשימה המתפרסמת מעת לעת – על ספק השער לספק אישור בהתאם .

6.15.1.4 כבלים /חיבורים/ שקעים חיצונים יהיו בלתי נגישים להולכי רגל/ נבדקים , יהיו מוגנים מפני רטיבות וליכלוך ויהיו עמידים בפני ונדליזים

6.15.1.5 השער יכלול את המרכיבים הר"מ :

6.15.1.6 פנל הצגה אנכי רב אזורי של האובייקטים המתכתיים אשר התגלו על גוף הנבדק.

6.15.1.7 יכולת ביצוע שינויים בכיול שער המגנומטר והתאמתו לנתוני שטח העבודה.

6.15.1.8 יכולת שינוי רמת הגילוי בהתאם לאוכלוסייה הנבדקת באופן מיידי ופשוט ללא צורך בכניסה לרשימת תפריטים ופעולות תכנות מסובכות.

6.15.1.9 כיול שער גילוי המתכות יהיה פשוט ידידותי ויאפשר ביצוע פעולות כיול באופן עצמאי ע״י קצין הבטחון או נציגו ללא צורך במעורבות החברה המתקינה. החברה המתקינה תספק מדידים מתאימים עפ״י רמת האיום המוגדרת ע״י משטרת ישראל.

6.15.1.10 שער מגלה המתכות יהיה מתוצרת CEIA PMD 2 elliptic plus או שווה ערך.

6.15.1.11 שער זה עומד בדרישות התקן NIG0601.02.

6.15.2 מכונת שיקוף:

6.15.2.1 מכונות שיקוף חפצים דו כיוונית המותקנת כחלק בלתי נפרד מנתיב הכניסה למבקרים, גודל המפתח של מנהרת השיקוף 64 ס״מ רוחב 43 ס״מ גובהה, כולל בדיקת קרינה ותשלום אגרות למשרד התמ״ת, כולל מערכת הזרקת איומים ותוכנות כנדרש.

6.15.2.2 המכונה תיהיה מאושרת לשימוש בגופים ממלכתיים , החברה תספק אישור לכך.

6.15.2.3 מוכנת השיקוף תיהיה מחברת rapiscan דגם 520 או שווה ערך.

6.15.2.4 צג המערכת יחובר בעמדת הבדיקה ויהיה חלק בלתי נפרד מעמדה זו.

6.15.2.5 מכונות השיקוף ימוקמו בכל נתיב כניסת אזרחים למתקן ועפ״י דרישת סגן ר׳ מערך סייבר חירום וביטחון במשרד האוצר.

6.15.3 שער נכים:

6.15.3.1 שער הכנף המיועד לשימוש נכים יחובר לבקרת הכניסות.

6.15.3.2 הפעלה חשמלית מעמדת השומר או באמצעות קוראי כרטיס.

6.15.3.3 המעבר יהיה מתוצרת GUNNEBO MAYOR דגם GLASSTILE GSS או שווה ערך מאושר .

6.15.3.4 המעברים יכילו נוריות סימון מקוריות של היצרן לסימון הרשאה או דחייה של תג.

6.15.3.5 השער יופעל לשני הכיוונים.

6.15.3.6 שער נכים ייפתח אוטומאטית בעת אזעקת אש .

6.15.3.7 הפעלה חשמלית מעמדת השומר או באמצעות קוראי כרטיס.

6.15.3.8 המעברים יכילו נוריות סימון מקוריות של היצרן לסימון הרשאה או דחייה של תג.

6.15.3.9 השער יופעל לשני הכיוונים.

6.15.3.10 השערים ייפתחו אוטומאטית בעת אזעקת אש .

6.15.4 כניסת מורשים ויציאה כללית - מעברים מהירים

6.15.4.1 יותקנו מעברים מהירים מסוג indoor במקומות שיקבעו ע"י המזמין ועל פי התוכניות העקרוניות.

6.15.4.2 המעברים המהירים יהיו כדוגמאת SPEED STILE FP-EV\BA של חברת Gunnebo או ש"ע שיאושר ע"י המזמין.

6.15.4.3 דרישות מהמעברים המהירים

6.15.4.3.1 רוחב מעבר – 55 ס"מ לפחות

6.15.4.3.2 חומר גוף – גוף נירוסטה 304. גימור לבחירת המזמין על פי האפשרויות שהיצרן מאפשר.

6.15.4.3.3 בטיחות – גלאים למניעת סגירה בעת מעבר, חיבור לרכזת האש ולחצן חירום ובטריה לגיבוי Fail-Safe.

6.15.4.3.4 נשלט חשמלית דו כיווני

6.15.4.3.5 קצב מעבר – כ 20 אנשים לדקה (באמצעות קורא קרבה)

6.15.4.3.6 המעברים יכללו נוריות חיווי למעבר מורשה

6.15.4.3.7 על המעברים המהירים ישולבו קוראי כרטיסי קרבה.

6.15.5 בקרת כניסה

6.15.5.1 תותקן מערכת בקרת כניסה בכל שלושת מעגלי האבטחה במתקן.

6.15.5.2 במעגל החיצוני :

6.15.5.3 בכניסה לחניונים יותקנו קוראי כרטיסים למורשי כניסה ללא בידוק.

6.15.5.4 בכניסות הראשיות, דלתות מילוט חיצוניות, שערים ופשפשים חיצוניים למתקן, יותקנו קוראי כרטיסים, אינטרקום לבקרה ומגנט לנעילה של 600 ק"ג או מנעול אלקטרו מכאני בעל כח נעילה זהה לפחות הניתנים לשליטה ממערכת ה - MMI בבקרת הביטחון ובעמדת המאבטח הקרובה.

6.15.5.5 בלובי המתקן תתוקן מערכת ספירה אוטומטית של מספר הנכנסים והיוצאים מהמתקן.

6.15.5.6 במעגל הפנימי :

6.15.5.7 במעגל הפנימי יותקנו אמצעי בקרת כניסה על כל דלתות הכניסה הראשיות ליחידות, חדרי התקשורת ומחשבים של המשרדים, חדרי שירות כללים כגון חדר חשמל ראשי טלפוניה ראשית וכו', דלתות המילוט של היחידות במידה ונמצאות בתוך שטח המשרד ולא בשטחים ציבוריים.

6.15.5.8 הפרדה בין שטחי ממשלה לשטחים פרטיים בכל דלת המקשרת בין שטחים ציבוריים לשטחים של המשרדים.

6.15.5.9 מתחם הביטחון של קב״ט הבניין וחדר הבקרה ימוגנו באמצעות בקרת כניסה בקרת פריצה טמ״ס ואינטרקום.

6.15.5.10 חדר בקרה ביטחון ראשי :

6.15.5.11 שרת מערכת בקרת הכניסה הראשי יותקן בחדר תקשורת למערכות ביטחון של חדר הבקרה הראשי. כמו כן יסופקו עמדות CLIENT למערכת בקרת הכניסה שיורחקו לשולחן הבקרה וישמש לצורך הגדרת משתמשים ומתן הרשאות, הנפקת תגים לבעלי תפקידים במתקן ומבקרים קבועים ותשלוט על כלל הפתחים והכניסות במתקן, באמצעים אלקטרוניים ומסכי מגע קלים לתפעול.

6.15.5.12 בנוסף תהיה יכולת מחדר הבקרה לשליטה על כל אחד ואחד מהפתחים ויתאפשר לפתוח כל אחד מהם לחוד או את כולם יחד בלחיצת כפתור אחת באמצעות ממשק HMI וכן באמצעות מערכת השו״ב, שלוחה נוספת של מחשב בקרת הכניסה תותקן בחדר הקב״ט .

6.15.5.13 קורא קירבה העובד בתדר MHz13.56 ותומך בתקן ISO 14443 type B בעל יציאת wigend 26, לקריאת נתונים מכרטיס תמו״ז של הממשלה. הקורא יתמוך בגרסה החדשה ביותר (3.1) של כרטיסי עובדי מדינה וכן בגרסאות ישנות יותר.. על הספק להוכיח יכולת קריאת נתונים בפרוטוקול המצויין לעיל, מכרטיס תמו״ז.

6.15.5.14 קורא קירבה העובד בתדר MHz13.56 ותומך בתקן ISO 14443 typeB מותאם לכרטיסי תמו״ז של עובדי ממשלה + משולב קורא ביומטרי.

6.15.5.15 יחידות פנל שליטה על שערים ודלתות באמצעות מערכת MMI – פנל – LCD שטוח ופנל עם מפסקים לגיבוי – ימוקם בעמדת הבידוק ומוקד הבקרה.

6.15.5.16 יסופקו בקרים לקוראי כרטיסי קרבה - כנדרש.

6.15.5.17 מערכת מגנולוק 600 ק״ג או כל מנעול אלקטרומכאני אחר בעל לפחות אותו כח נעילה- לאזורים המפרדים בין שטח ציבורי לשטח המבנה בהיקף המבנה ובהתאם לדרישות סגן ר׳ מערך סייבר חירום וביטחון במשרד האוצר.

6.15.5.18 מנעולים חשמליים+ ספקי כוח, מתוצרת FF או ש״ע

6.15.5.19 זמזם דלת מוטרדת בדלתות שיוגדרו.

6.15.5.20 מפסקי סף מגנטים בדלתות המבוקרות, מתוצרת סנטרול או ש״ע ומפסקי סף HD לדלתות כבדות ושערים.

6.15.5.21 לחצני פתיחה – No-Touch שאינם דורשים מגע פיזי לפתיחת דלת

מבוקרת. וקופסאות ניפוץ.

6.15.5.22 כבילה התקנה ואינטגרציה .

6.15.5.23 עמודי תור מסוג "בלטרק" או שווה ערך הכולל סרט נשלף עם כיתוב.

6.15.5.24 בכניסות המבקרים בלוביים הראשים ובכניסות לחניונים יהיה שימוש במערכת לזיהוי מבקרים תוך כדי תנועה העושה שימוש בטכנולוגיה של זיהוי פנים, תנועה, קול וכדומה.

6.15.5.25 כל דלתות האש המבוקרות בפרויקט יותקנו על פי תקן 1212 כולל אבזרי בקרה נדרשים על פי דרישות התקן. הדלתות יסופקו על ידי ספק הדלתות לרבות אבזרי הקצה בדלת והפרזול הנדרש (מנעולים, ידיות בהלה, מעבירי מתח, מחזירי שמן, מגע מגנטי וכו'). הקבלן יחבר ויפעיל יחידות קצה אלו אל המערכת וייקח אחריות מלאה על תפקוד המערכות האלקטרוניות בדלתות למרות שסופקו והותקנו על ידי אחרים.

6.16 מערכת גילוי פריצה לחצני מצוקה וקופסאות ניפוץ

6.16.1 גילוי פריצה:

6.16.1.1 תותקן מערכת גילוי פריצה על בסיס גלאי נפח ומגעי סף מיקום הגלאים השונים יופיע כאמור ע"ג תרשימים בתוכנת הביטחון במרכז שליטה ובקרה לביטחון.

6.16.1.2 רכזות המערכת תוצבנה בהתאם לחלוקת אזורי יום/לילה בחדרי התקשורת בסמוך לאזור.

6.16.1.3 יותקנו סירנות חיצוניות ופנימיות .

6.16.1.4 גלאי הנפח יותקנו באזורים רגישים כגון : ארכיונים, חדרי תקשורת פתחים חיצוניים,

6.16.1.5 באיזורים ציבוריים יותקנו גלאי אנטימאסק.

6.16.1.6 אזורי הכניסה לבנין ולמבואות בקומות ובכניסות למחלקות ומשרדים רגישים, כעקרון כל משרד/קומה יהווה אזור עצמאי במערכת.

6.16.1.7 על קירות חיצוניים בהם יש חלונות לחדרים רגישים יותקנו גלאים חיצוניים א"א אקטיבי פרוט הקומות והחדרים יסוכם בנפרד.

6.16.1.8 מגעי סף יותקנו בדלתות החדרים ובכניסות לאזורים שיוגדרו כרגישים.

6.16.1.9 ביציאה מכל אזור ממודר יוצב KB להכנסת האזור ממצב יום ללילה ולהפך.

6.16.1.10 מיקומם המדויק של הגלאים השונים יקבע ע"ג תוכניות האדריכל תוך התייחסות להיבט הפונקציונאלי הביטחוני.

6.16.1.11 בחלונות קומת הקרקע לחדרים מסווגים ברמת בטחון גבוהה נדרשת קבלת התראה מוקדמת ואמצעי פיזי להשהיה בפני חדירת גורמים דרכם.

6.16.1.12 בכל היקף הבניין באזורים בהם יש גישה לחלונות עד לגובהה של 5מ' יותקנו גלאים חיצוניים א,אקטיביים.

6.16.1.13 בכל לובי קומתי באזורי המעליות וחדרי המדרגות ומדרגות המילוט יותקנו גלאים פאסיביים.

6.16.1.14 בכל דלת כניסה ראשית למתקן ו /או מילוט יותקנו גלאי סף מגנטי בכל דלתות הכניסה למשרדים כניסה לחדרי תקשורת, כניסה לחדרי מחשב יותקנו גלאי סף בדלת בתוך כל חדר כאמור יותקן גלאי נפח או 360 מעלות.

6.16.1.15 כספת נשק תמוגן עפ"י הנחיות המשטרה ומשרד הפנים,.

6.16.1.16 חדרי ביטחון בנושא אבטחת מידע ימוגנו עפ"י הנחיות שב"כ.

6.16.1.17 גלאים נוספים יותקנו במקומות בהם נדרש עפ"י הנחיות קב"ט היחידה וזאת לאחר תכנון סופי של שיבוץ החדרים במתקן.

6.16.2 לחצני מצוקה:

6.16.2.1 לחצני מצוקה באזורים שונים בבניין יותקנו עפ"י דרישות בטחון שיוגשו ע"י קב"טי היחידות המאכלסות לאגף הביטחון באוצר, ההתקנה בצורה מוסתרת ובמקומות שיאפשרו הפעלה בצורה נוחה, תוך מניעת אפשרות הפעלת האזעקה בשוגג.

6.16.2.2 לחצני המצוקה יהיו ידניים עם נטרול ע"י מפתח , דבר שיחייב הגעת המאבטח למקום פיזית , ע"מ לנטרל האזעקה.

6.16.2.3 האינדיקציה להפעלת הלחצנים תגיע למאבטח בעמדת הכניסה ולמרכז שליטה ובקרה לביטחון ההתראה תהיה קולית וויזואלית ע"ג התרשים לרבות סדר פעולות המאבטח.

6.16.2.4 הלחצנים בעמדות בקרה יפעילו אוטומטית גם מצלמה הממוקמת בעמדה ואשר תשדר מיידית תמונה לחדר שליטה ובקרה לביטחון .

6.16.2.5 מיקום מדויק של לחצני המצוקה ואפיונם יקבע בהמשך ובהתאם לדרישות הפונקציונאליות של המשרדים .

6.16.3 קופסאות ניפוץ – הגנה אלקטרונית:

6.16.3.1 בכל יציאת החירום יהיו מפתחות/כפתורים לפתיחת דלתות בחרום בתוך קופסאות ניפוץ הקופסה תאובטח כך שברגע הניפוץ תתקבל אינדיקציה ע"ג צג מחשב בתכנת הביטחון .

6.16.3.2 מיקום קופסאות הניפוץ יקבע ע"ג תכניות האדריכל, ובהתאם

לדרישות הפונקציונליות.

6.16.3.3 הכל עפ"י התקנים הרלוונטיים באישור אגף הביטחון באוצר.

6.16.3.4 במקום בו מותקנת גם מצלמה תוקפץ התמונה בחדר הבקרה הראשי.

6.16.4 **כללי:**

6.16.4.1 מערכת גילוי פריצה כוללת בתוכה את האלמנטים הבאים:

6.16.4.1.1 גלאי נפח א"א אקטיביים חיצוניים.

6.16.4.1.2 מפסקי סף מגנטים, מתוצרת סנטרול דגם 1087 TW-H או ש"ע.

6.16.4.1.3 גלאי א"א פסיביים פנימיים, מתוצרת ויסוניק או ש"ע.

6.16.4.1.4 גלאי שבר זכוכית, מתוצרת ויסוניק או ש"ע.

6.16.4.1.5 גלאי מכני כדורי תוצרת חברת ADEMCO דגם 956 או שווה ערך .

6.16.4.1.6 גלאי תקרתי 360 מעלות.

6.16.4.1.7 גלאי כספת משולב אור זעזועים וחום + מפסק בכספת.

6.16.4.1.8 גלאי זיהוי מקדים לזיהוי חל"כ אשר ימוקם במערכות האיוורור.

6.16.4.1.9 רכזות גילוי פריצה ל- 256 נק' – בכמות שתאפשר חיבור כל אביזרי הקצה + רזרבה של 30%.

6.16.4.1.10 מפתחות או לחצנים לדלתות מילוט+ קופסאות ניפוץ מבוקרות.

6.16.4.1.11 מערכת איסוף התראות ובקרת כניסה ותקשרות – בנויה כמערכת רב משתמשים מחשב ויחידות תצוגה – בנויה כמערכת רב משתמשים (עד 5 עמדות) – 2 עמודת.

6.16.4.1.12 KB להעברת אזורים ממצב יום/לילה באזורים ממודרים.

6.16.4.1.13 כבילה, התקנה ואינטגרציה.

6.17 מערכת כריזה כללית

6.17.1 פירוט:

6.17.1.1 מערכת הכריזה תאפשר להתריע על מצב חירום במכלול השלם של הבניין תתאפשר חלוקה לאזורים וכל קריאה במערכת הכריזה תשמע ברחבי הבניין כולו, או עפ״י בחירת הכורז / מאבטח.

6.17.1.2 הפעלת המערכת תתאפשר באחת או יותר מהאפשרויות הבאות : מיקרופון, אינטרקום ייעודי, חיוג ממכשיר הקשר הנישא או מכל טלפון בבניין באמצעות קוד.

6.17.1.3 הגורמים אשר יתאפשר להם לכרוז על מצב חירום הנם :

6.17.1.4 חדר בקרת ביטחון.

6.17.1.5 מאבטחים בעמדת השמירה בכניסה הראשית.

6.17.1.6 העובד בחדר בקרת מבנה (בנא״מ) באירועי בטיחות בתאום עם מרכז הבקרה לביטחון.

6.17.1.7 מוקדי משנה.

6.17.1.8 מיקום מדויק של הרמקולים ושאר המערכות הנלוות יפורטו ע״ג התוכניות האדריכליות ותכנית התקרות.

6.17.1.9 רכזת מערכת השליטה תמוקם במוקד הבקרה ותוכל להפעיל את הכריזה עפ״י בחירה בין כלל הקומות או כל קומה בנפרד.

6.17.1.10 המערכת תכלול את האמצעים הבאים :

6.17.1.10.1 רמקולים

6.17.1.10.2 מגברים MILBANK או TOA או ש״ע 100 ואט .

6.17.1.10.3 מיקרופונים.

6.17.1.10.4 פנלי שליטה אזורי כריזה .

6.17.1.10.5 מסד בקרה ומיתוג + מוניטור – מבוצע למתן שרות ממספר מוקדים השולטים על חלקי בניין שונים, עפ״י חלוקה פונקציונלית + הפעלה מרכזית.

6.17.1.10.6 מוקדי הפעלה משניים לכריזה בדלתות יציאת החירום של המבנה .

6.17.1.10.7 כבילה התקנה ואינטגרציה.

6.18 מוקד הבקרה והשליטה

6.18.1 מידע כללי :

6.18.1.1 מרכז שליטה ובקרה לביטחון ישמש כעמדת בקרה מרכזית לביטחון המרכז ישלוט על מערכות הביטחון והבקרה השונות ומערכות התקשרות מתח נמוך חדר זה יוגדר כממודר, והכניסה אליו תהיה מבוקרת באמצעות קורא כרטיסים (ראה אפיון בקרות כניסה).

6.18.1.2 מרכז שליטה ובקרה לביטחון יאויש 24 שעות ביממה התראות ממערכות הביטחון ותקלות ממערכות בקרת המבנה תתקבלנה בחדר זה במשך כל שעות היממה, במידה ועמדה זו לא תאויש 24 שעות תחובר המערכת למרכז בקרה חיצוני .

6.18.1.3 עמדת הבקרה בפרוייקט זה תהיה במקום הכי מוגן במבנה ותמוגן בהתאם לרמת המיגון המקסימלית הנדרשת לפעילות בחירום של היחידות המאכלסות את המבנה . בקומת הכניסה הראשית ימוקם חדר בקרה חלופי למקרה בו יהיה צורך לפנות את חדר הבקרה הראשי כחלק ממתחם הביטחון יש לקחת בחשבון פעילות בעמדה זו ע"י 2- 3 אנשים .

6.18.1.4 שולחן הבקרה יתוכנן כך שכל מערכות הביטחון המפורטות במפרט זה ירוכזו לשולחן התראות מהמערכות הבאות :

6.18.1.4.1 מערכת ביטחון שו"ב הכוללת מחשב מערכת פריצה, טמ"ס, ובקרת כניסה.

6.18.1.4.2 מערכת בטיחות – גילוי אש.

6.18.1.4.3 מערכת הכריזה.

6.18.1.4.4 מערכת בקרת מעליות- מחשב+ אינטרקום מעליות.

6.18.1.4.5 מחשב בקרת מבנה.

6.18.1.4.6 מערכת הקלטה (אודיו) שוטפת בתוך מוקד הבקרה לטובת יכולת ביצוע תחקירים.

6.18.1.4.7 HMI.

6.18.1.4.8 מערכת קשר.

6.18.1.4.9 מחשב מנהלתי לאינטרנט.

6.18.1.4.10 מחשב שליטה על תוכנת ביטחון – "קשת" חיבור לרשת האוצר בקו מאובטח של בזק (קו ISDN או שווה ערך) עפ"י

הנחיות ממונה אבטחת מידע במשרד האוצר.

6.18.1.5 צורת השולחן וגודלו יובאו לאישור סופי של אגף הביטחון של משרד האוצר לפני ביצוע כולל חומרי גמר של השולחן.

6.18.1.6 חדר ציוד (צמוד לחדר בקרה) כ-10 מ״ר.

6.18.1.7 בחדר הבקרה יותקנו 2 קוים ישירים שלא דרך המרכזייה.

6.18.1.8 כן יותקנו 3 שלוחות טלפון חכם ״שחור״+ שלוחת טלפון וכן קו לפקס.

6.18.1.9 פלאפון לגיבוי .

6.18.1.10 קשר מבצעי עם חיבור לאנטנה בגג המבנה עבור מערכת הקשר הייעודי של המתקן.

6.18.1.11 תשתית + אנטנה בגג המבנה עבור מערכת קשר ניצן.

6.18.1.12 תשתית + אנטנה עבור מערכת טלפוניה לווינית .

6.18.1.13 נלני״ם נוספים יסוכמו במידת הצורך .

6.18.1.14 שולחן בקרה.

6.18.1.15 בשולחן יותקנו התקנים של כלל המערכות. באחריות היזם לבצע תאומים ואינטגרציה עם כל הגורמים הקשורים בשולחנות כולל האדריכל יועץ המערכות , יועץ החשמל וכו׳.

6.18.1.15.1 תיאור העמדה :

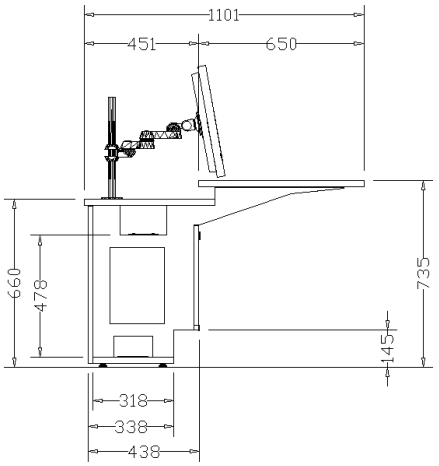
עמדות העבודה הייעודיות, יהיו מערכות מודולארית מושלמות לחדרי מוקד ובקרה עפ״י התכנון. המערכות יכללו את כל המרכיבים ותת המרכיבים הנדרשים לעמדות מסוג זה ויהיו מתוצרת חברה המתמחה בציוד מסוג זה.

6.18.1.15.2 מבנה העמדה :

- כל עמדה תכלול את הרכיבים ותת המכלולים המפורטים להלן :
- שלד מתכת מודולארי, צבוע בתנור בצבע RAL9006 .
- בסיס מתכת מסיבי המהווה חלק מהשלד , המהווה בסיס להתקני תליית מסכים – צבע כמו הבסיס.
- בסיס תליית המסכים יתאים לתלייה של 2 מסכים לפחות בגודל ״18-22, במפלס אחד.
- מכלול טכני לתקשורת ומחשבים , משולב בשולחן , כולל ארון מתכת עם התקנים להתקנת עד 4 מחשבים , ציוד תקשורת וציוד אלקטרוני ייעודי.
- המכלול הטכני יכלול דלתות מאווררות עם פתיחה מהחזית לצורך שרות.
- הכנה להתקנים ״19 , כולל הכנה של פנלים ל-RJ45 לתקשורת ולציוד ייעודי.
- התקני חשמל הכוללים קופסאות פיצול ושקעים להזנת מחשבים ומסכים וציוד אחר, כולל

4 שקעי UPS ו-2 שקעי שרות למשתמש.

- כל האינסטלציה הנדרשת חשמל ותקשורת, מהמכלול הטכני למסכים.
- מערכת זרועות מושלמת לתליית מסכים מתוצרת LEVICO או שווה ערך, הכוללים 3 דרגות חופש כ"א והתקנים להתקנת מסכים שטוחים בין "19 ל- " 22 בתקן VESA.
- משטחי עבודה ברוחב 1.10 מ' ובעומק 0.90 מ' בגימור עפ"י בחירת המזמין . סך כל אורך רוחב השולחן יהיה על פי ממדי החדר וכמות המערכות ועמדות ההפעלה שיגדיר הלקוח (עד 8 מטר אורך שולחן).
- משטחי גימור עפ"י בחירת המזמין בקצה של כל שורת שולחנות.
- כל התעלות והחיווט יהיו נסתרים בתוך המכלול הטכני ויהיו נוחים לגישה.
- בכל עמדה ניתן יהיה להתקין ארונית מגרות תואמת.



פרט/חתך עקרוני שולחן הבקרה

פרט עקרוני לזרוע מסך להתקנה על שולחן הבקרה

- להתקנת מסך מחשב בתצורת חיבור בסטנדרט VESA
- בעל זרוע רב מפרקית בעלת אפשרות הטיה לכל כיוון

- התקן לחיבור לשולחן הבקרה אינטגרלי

פרט עקרוני לזרוע עבור 2 מסכים להתקנה על שולחן הבקרה

- להתקנת שני מסכי מחשב בתצורת חיבור בסטנדרט VESA
- בעל זרוע רב מפרקית בעלת אפשרות הטיה לכל כיוון

6.18.2 מולטימדיה בחדר הבקרה:

6.18.2.1 בחדר הבקרה יותקן קיר וידאו בעל לפחות 8 מסכים בגודל 55 אינץ ובעלי קו תפר של 5.5 מ״מ לכל היותר.

6.18.2.2 כחלק ממערך המולטימדיה יותקנו מערכת מטריצה דיגיטלית בעלת יכולות קיר וידאו אינטגרליות ובעלת מספר כניסות ויציאות המותאם לכמות מסכי הקיר וידאו מצד אחד, ומאידך לכמות המערכות ומקורות הוידאו אותן יש להקרין על גבי קיר הוידאו. לבקר תהיה יכולת הצגת מקורות IP כולל מחשבים ומצלמות. לבקר קיר הוידאו יהיו לפחות 16 יצאות ו 16 כניסות

6.18.2.3 מערך המולטימדיה יכלול בקר מרכזי שישלוט על בקרי קיר הוידאו והמטריצה הדיגיטלית ושאר מרכיבי המולטימדיה באמצעות מסך מגע בגודל 10״ לפחות כדוגמת מערכת CRESTRON או שוו״ע.

6.18.2.4 מערך המולטימדיה יכלול מערכת הגברה וDSP, מערכת מיתוג והרחקת מחשבים מחדר התקשרות המרכזי לביטחון לשולחן הבקרה.

6.18.2.5 יעשה שימוש בטכנולוגיה דיגיטאלית בלבד (לא יתקבלו מחברי VGA וחיבורים אנלוגי – למעט יכול חיבור מחשב אורח באמצעות מחבר VGA בנוסף לאפשרות חיבור באמצעות HDMI.

6.18.2.6 כל שרתי ומחשבי כלל המערכות יסופקו עם כרטיסי מסך בעלי יצאות דיגיטליות בלבד לחיבר דיגיטלי למערך המולטימדיה.

6.18.2.7 במידת הצורך ישולבו מרחיקי KVM, מרחיקי אות וידאו HDMI\DVI

6.18.2.8 יסופק מסך מגע ובו יופיע ממשק משתמש אותו שיאפשר שליטה מלאה על כלל האביזרים בצורה פשוטה ונוחה. על היזם להציג מסכי ממשק

משתמש לאישור המזמינה. בכל מסך יופיע לוגו מדינת ישראל וסימנים נוספים לבחירת המזמין. מסך המשתמש יאפשר מעבר בין פריסטים של ברק קיר הוידאו וכן שליטה כלל המסכים כולל כיבוי והדלקה.

6.18.2.9 בכל ארון תקשורת לביטחון יותקן מסך טכנאי משולב ממתג KVM לשליטה על כלל המחשבים המותקנים בארון התקשורת.

6.18.2.10 מוקדי בקרה יוצבו במקומות הבאים :

6.18.2.11 מוקד ביטחון ראשי ימוקם בסמוך לחדר מצב בקומת מרתף לחירום.

6.18.2.12 כניסה ראשית עמדת בקרה משנית לשליטה על האמצעים בלובי הכניסה ועל דלתות הכניסה והסבסבות יותקן בשולחן כחלק בלתי נפרד ממערך הבידוק הביטחוני.

6.18.2.13 מוקדי משנה באזורים ממודרים – עפ״י דרישות אגף הביטחון באוצר.

6.18.2.14 עמדת אבטחה באזור פריקה וטעינה של המתחם (ראה אפיון נפרד).

6.18.2.15 כניסות לחניון עמדת בקרה משנית (ראה אפיון נפרד).

6.18.3 מחשבי הביטחון:

6.18.3.1 מחשבים אלו יחוברו ברשת עם אפשרות להכניס לתוכה תוכנת מבקרים ורשימות עובדי המשרדים השונים תוכנת הקב״ט כוללת אפשרות קבלת תמונה פיזית של המבנה (המערכת מפורטת בהמשך).

6.18.3.2 מערכת 360 (שמור) ומערכת דו״ק (סודי) : על היזם להכין את התשתית עבור מערכות אילו שימוקמו בחדר מוקד הבקרה ,חדר מוקד חלופי, חדר קב״ט וס. קב״ט.

6.18.3.3 מערכת לזיהוי מוקדם של רעידת אדמה

6.18.3.4 מערכת לקבלת אינדיקציה לאירוע רעידת אדמה תותקן במתקן לצורך קבלת התראה כאמור. המערכת תתריע ותוציא הודאה למרכז הבקרה על קבלת אינידקציה לרעידת אדמה המערכת צריכה לעמוד באישורים מהגורמים המקצועיים הרלוונטיים ובכלל זה המכון למחקרי נפטוגיאופיזיקה בישראל, המכון הטכנולוגי לישראל הטכניון.

6.18.3.5 איפיון המערכת :

6.18.3.5.1 גודל 610*320*110 מ״מ מיועד להתקנה על קיר בתוך מבנה.

6.18.3.5.2 משקל 45 ק״ג

6.18.3.5.3 מתח הזנהVCD 1.5A/12

6.18.3.5.4 3 גלאים

6.18.3.5.5 מעגל אלקטרוני לבקרה ושליטה מבוסס מיקרו פרוססור להפעלת מערכות נורית לחיווי תכולת מתח.

6.18.3.5.6 צופר מקומי

6.18.3.5.7 יחידת השמעה למערכת כריזה.

6.18.3.5.8 מצבר פנימי לגיבוי במקרה נפילת מתח.

6.18.3.5.9 טמפרטורת עבודה 0-60 מעלות.

6.18.4 מערכת כרוזית לדיווח על נפילות טילים

6.18.4.1 מערכת לקבלת אינדיקציה מוקדמת לנפילות טילים.

6.18.4.2 המערכת נדרשת להיות מסוכרנת למערכת הכריזה.

6.19 תוכנת ביטחון – שו"ב

6.19.1 פירוט:

6.19.1.1 תוכנת הביטחון הנה תוכנה ייחודית למערך האבטחה ותהיה מנותקת מרשתות המחשוב של המשרדים השונים תוכנת הביטחון פועלת כמערכת רב משתמשים).

6.19.1.2 היזם יתקין שרת מרכזי למערכת השוב כולל שרת "גיבוי חם". בזמן נפילת השרת המרכזי יעלה השרת גיבוי ללא פגיעה בתפקוד המערכת.

6.19.1.3 למערכת השו"ב יהיו ממשקים לכלל תתי המערכות ברמת IP

6.19.1.4 לתוכנה זו יחוברו כל מערכות הביטחון של המבנה התוכנה תקבל את כל האינדיקציות מכל מערכות הביטחון.

6.19.1.5 עם קבלת אינדיקציה יוצג על המוניטור סדר פעילות למאבטח לכל אינדיקציה.

6.19.1.6 עם קבלת אינדיקציה מיחידות קצה בהן מותקנת טלוויזיה, תתקבל תמונת האזור ע"ג המוניטור וסדר פעולות למאבטח לאותה התראה לתוכנה זו יוכנסו כל תרשימי המבנה (מחולקים עפ"י קומות) עם כל האמצעים הקיימים בכל נקודה (גלאי נפח, מגעי סף מגנטיים, לחצני מצוקה , גלאי א"א אקטיביים, מפתחות קופסאות ניפוץ ועוד).

6.19.1.7 תצוגה – שימוש בממשקים גרפיים צבעוניים מתקדמים, עריכת מבנה המסכים תהיה פשוטה ע"י בחירת הצורה ומיקום המסכים יכללו תצוגת רקע קבועה וצורות המשתנות בהתאם לערכים הנמדדים בשטח.

6.19.1.8 תפעול – ע"י מקשים או עכבר.

6.19.1.9 היסטוריה – תוך כדי פעולה שוטפת תירשום המערכת את כל הפעולות המתבצעות.

6.19.1.10 דו"חות המערכת תכלול מחולל דו"חות שיאפשר בכל זמן להציג, ולהדפיס דוחות על סמך מידע שנצבר מהעבר מבנה הדו"ח, תוכנו

והתקופה אליה הוא מתייחס יקבעו באופן פשוט.

6.19.1.11 גרפים – בנוסף לדוחות המילוליים תפיק המערכת תצוגה גרפית של 16 נתונים שונים.

6.19.1.12 בכל חלון בחירת הנתונים ומשך הזמן המוצג ניתנים לקביעה.

6.19.1.13 רשת – המערכת תותקן בתצורה מבוזרת ברשת מקומית בסביבת CLIENT SERVER בפרוטוקול תקשורת TCPIP.

6.19.1.14 ממשק לבקרים – המערכת תפעל בקצב דגימה של 50 אלפיות השניה, מול ממשקי בקרים.

6.19.1.15 מערכת הפעלה המערכת תפעל מחשבי PC – ותואמיו מערכת הפעלה חלונות XP .

6.19.1.16 הרשאות – נדרשות 32 אפשרויות הרשאה, קישור רמת ההרשאה ליכולת ההפעלה והצגת המסמכים.

6.19.1.17 אובייקטים סטטיים ודינמיים – המערכת תכלול ספריה של CLUSTERS הקשורים לכתובות, התראות ועוד ניתן יהיה להוסיף ולעדכן אובייקט ל- CLUSTER.

6.20 מפות סינופטיות

6.20.1 פירוט:

6.20.1.1 במרכז שליטה ובקרה לביטחון תוצב מפה סינופטית משולבת בתכנת הביטחון על גבי מחשב הביטחון.

6.20.1.2 כן יוצב בחדר זה מחשב בקרת מבנה אשר בו תיכלל מפה סינופטית לקבלת.

6.20.1.3 אינדיקציה במקרה של שריפה, הפעלת לחצני אש, התראות תקלה ממערכות אלקטרו-מכניות מיזוג אויר, חשמל , אינסטלציה גנרטור מקומי, תאורה ומעליות מפה זו תהיה מקבילה לזו שבבנא"מ / תחזוקה. וניתן יהיה לקבל את האינדיקציות לצורך העברתם לממונה תחזוקה במבנה.

6.21 מערכת אינטרקום

6.21.1 פירוט:

6.21.1.1 תותקן מערכת אינטרקום IP – שתחובר לרשת הייעודית למערכות הביטחון. מערכת ייעודית לדלתות מבוקרות ואזורים נקודתיים אשר יוגדרו ע"י סגן ר' מערך סייבר חירום וביטחון במשרד האוצר.

6.21.2 דרישות מערכת:

6.21.2.1 מערכת האינטרקום תאפשר תקשורת קולית איכותית ומהירה בין כל יחידות הקצה בשיטת "Full Duplex Hands-Free" (שיחה ללא מגע יד)

6.21.2.2 המערכת תאפשר קשר מלא בין כל המשתמשים ללא מגבלות התקשרות.

6.21.2.3 המערכת תתבסס על טכנולוגיית IP ותאפשר חיבור של יחידות קצה (סניף) אנלוגי ויחידות קצה IP בצורה "שקופה" במתג משותף ללא ממירים ומתאמים.

6.21.2.4 יחידות קצה מבוססות IP יכילו מעבד קול דיגיטלי מובנה שיאפשר וויסות אוטומטי והפקת רמת שמע אחידה, ברורה וללא עיוותים.

6.21.2.5 יחידות קצה IP יאפשרו ע"י הגדרות תוכנה לבצע:

א. סינון/ביטול רעשי רקע והגברת מובנות הדיבור באזורים רועשים.

ב. גלאי קול להפעלה וחיוג ע"י רעש כגון: צעקה, קולות נפץ וכו'.

ג. ביטול משוב אקוסטי (Feedback) במצב תקשורת דו-כיוונית מלאה.

6.21.2.6 המערכת תכיל מתג (רכזת) מרכזי, דיגיטלי המבוקר על ידי מעבד ראשי בטכנולוגית VOIP ויכלול את האפשרויות והתכונות הבאות:

א. מערכת רב ערוצית ומודולארית עם אפשרות לפריסה מבוזרת וגמישה. המערכת תאפשר הרחבה ואפשרויות קישור באמצעות:

(1) קישור והרחבה ברשת IP.

(2) קישור והרחבה ברשת E1/T1

(3) קישור והרחבה בתשתיות נחושת נל"ן, סיבים אופטיים וציוד ריבוב.

ב. המערכת תאפשר ניצול של 30 ערוצי דיבור, בקישור והרחבת רכזות.

6.21.3 אינטגרציה ושילוב מערכות.

6.21.3.1 המערכת תכיל ממשקים ואפשרויות אינטגרציה למערכות כגון:

א. מערכת טלוויזיה במעגל סגור.

ב. מערכת גילוי פריצה ובקרות כניסה.

ג. מערכות שליטה ובקרה ממוחשבות.

6.21.3.2 המערכת תאפשר שימוש בממשקים ובמתאמים עם יכולות חיבור ל:

א. מפסקים/מתגים, ממסר "מגע-יבש".

ב. פרוטוקול סריאלי RS-232.

ג. פרוטוקול TCP/IP.

ד. VoIP שמע ואיתות בפרוטוקול SIP

ה. קוי טלפון

6.21.4 יחידות קצה

6.21.4.1 יותקנו יחידות קצה שולחניות עם ובלי מסך צבעוני

6.21.4.2 יותקנו יחידות קצה קיריות בעלות יכולת התקשרות ליחידה בודדת ויכולת בחירת שלוחה באמצעות גלילת אפשרויות

6.21.4.3 במוקד תותקן יחידה ייעודית למוקד בקרה.

6.21.4.4 יותקנו יחידות קיר בעלי מצלמה וללא מצלמה מובנית.

7 שלבי ההכנות לעבודה

7.1 שלבי ההכנות לעבודה

7.1.1 בדיקת התכנות - שלב זה יחולק לשלשה שלבים:

7.1.1.1 שלב לימוד הדרישות - הקבלן ילמד את דרישות המפרט, יברר כל הפרטים, ילמד את השרטוטים ומגבלות האדריכלים והמתכננים השונים, ויגיש שאלות והבהרות במידה וישנן.

7.1.1.2 שלב הצגת התכנון – בשלב זה מתכנניו של הקבלן יבצעו תכנון מלא של המערכת עפ״י הדרישות והמגבלות שנלמדו בשלב הקודם ויגישו ללקוח וליועציו הרלוונטיים את התכנון לאישור.

7.1.1.3 שלב הצגת המערכות והאמצעים (באם יידרש ע״י המזמין) - בשלב זה יזמן הקבלן את המזמין ונציגיו למפעלו, יציג את המערכות והאמצעים שברצונו להציע כולל פתרונות כלליים - לאישור. כמו כן, יצביע הקבלן על פרויקטים דומים שביצע ויארגן סיור התרשמות למזמין או לבא כוחו באחת המערכות שהותקנו על ידו.

7.1.2 בדיקה ראשונית:

7.1.2.1 טרם התקנת המערכת באתר, ובהתאם לשיקולי המזמין תיבדק המערכת בשלמותה או בחלקה במפעל הקבלן, עפ״י ספר בדיקות של היצרן ולפי שיקול דעת המזמין.

7.1.2.2 המערכת תותקן באתר רק לאחר אישור הבדיקה במפעל, או ויתורו של המזמין על הבדיקה זו.

7.1.2.3 המזמין יהיה רשאי לבדוק כל מרכיב במערכת הכוללת אצלו עפ״י דרישה ולפי שקולו בלבד. מרכיבים אלו יותקנו באתר רק לאחר קבלת אשורו של המזמין.

7.1.3 בדיקות המערכת:

7.1.3.1 במהלך פיתוח מערכת השליטה והבקרה בפרויקט, תערוך החברה הפעלה של המערכת במפעלה. ההפעלה תכלול:

7.1.3.1.1 כל פונקציות השליטה והבקרה כנדרש במכרז.

7.1.3.1.2 חיבור לרשת התקשורת המקומית.

7.1.3.1.3 התחברות והפעלה של כל תת-המערכות המקושרות לשליטה

ולבקרה.

7.1.3.2 הקבלן יבצע בדיקות קבלה בהשתתפות המפקח/המזמין. ציוד בדיקה, אביזרים וכלי עבודה הנדרשים לביצוע הבדיקות יסופקו ע״י הקבלן ועל חשבונו.

7.1.3.3 בדיקות הקבלה יתבצעו באתר ההתקנה בתום עבודות ההתקנה.

7.1.3.4 המפקח/המזמין רשאי לבקר ולפקח במעבדות הקבלן לאורך כל שלבי הייצור בכל עת וזאת לאחר תאום עם הקבלן.

7.1.3.5 בדיקות הקבלה תהיינה ויזואליות, חשמליות, מכניות ותפעוליות ותבוצענה בהתאם לדרישות במפרט זה ובהתאם למערך בדיקה שיוכן ע״י הקבלן.

7.1.3.6 כל הבדיקות לכל אחת מן המערכות כולל מערכים יוגשו לאישור המזמין.

7.1.3.7 המזמין רשאי לשנות את מערכי הבדיקות שיוגשו לאישורו ע״י הקבלן וכן להוסיף עליהם בדיקות נוספות על המוצע, במטרה להבטיח בדיקה מלאה, עמידות ברמת פריט בודד והמערכת כולה בדרישות.

7.1.3.8 המערך שיוכן ע״י הקבלן לכל פריט במערכת יכלול לפחות את הטורים הבאים:

7.1.3.8.1 מס׳ סידורי.

7.1.3.8.2 מהות הבדיקה.

7.1.3.8.3 פירוט הבדיקה.

7.1.3.8.4 ערך צפוי לתוצאה (לכל נתון שייבדק).

7.1.3.8.5 ציוד בדיקה נדרש.

7.1.3.9 קבלן יגיש למפקח/מזמין מערך בדיקות מלא לכל פרטי כל המערכות הנדרשות במפרט/חוזה זה וחתום ע״י מבקר פנימי של הקבלן, הנ״ל (המבקר) יאושר ע״י המזמין. רק לאחר שיתוקנו הליקויים שמצא המבקר תבוצע בדיקת הקבלה הראשונית של המפקח/מזמין.

7.1.3.10 לאחר בדיקת הקבלה הראשונית תוגש לקבלן רשימת ליקויים (במידה ויהיו). הקבלן מתחייב לתקן ליקויים אלו תוך 3 ימים מהעברת הרשימה לידיו. בתום 3 ימים תעשה בדיקת קבלה ראשונית נוספת במידה ותוצאות הבדיקה יתאימו לדרישות מפרט זה ולמערך הבדיקות תחל תקופת ההרצה ולאחריה תקופת האחריות (הבדק).

7.1.4 תקופת הרצה

7.1.4.1 בתום בדיקות הקבלה הראשוניות של המערכת ע״י המפקח תחל תקופת הרצה.

7.1.4.2 תקופה זו תימשך 6 חודשים.

7.1.4.3 במשך תקופת ההרצה מפעילי המערכת (נציגי המזמין) יתפעלו את המערכת, ילמדו את תכונותיה ויסיקו מסקנות.

7.1.4.4 ליקויים ודרישות לשיפורים שיתגלו במשך תקופת ההרצה ע"י המפקח/המתכנן יועברו לידיעת הקבלן שבאחריותו לתקנם באותו תהליך ובמועדים שהוגדרו במפרט זה.

7.1.4.5 בתום תקופת ההרצה ותיקון הליקויים תבוצע בדיקת קבלה סופית של מערכת.

7.1.4.6 בתום בדיקות הקבלה הסופיות זו תחשב המערכת כגמורה ותחל תקופת האחריות (תקופת הבדק).

7.1.4.7 תשומת לב הקבלן מופנית לכך שחלק מן הציוד יופעל וישמש את המזמין גם לפני הקבלה הרשמית פרק זמן זה לא יילקח בחשבון בשום אופן לחישוב תחילת האחריות/תקופת הבדק.

7.1.5 הגדרת סיום עבודה

7.1.5.1 במידה ותשארנה יחידות קצה לא מחוברות, מסיבות שלא תלויות בקבלן, המפקח והמזמין - והם בלבד, יחליטו/יודיעו על מועד סיום העבודה.

7.1.5.2 במקרה זה סיום העבודה יהיה רק לאחר שהקבלן יבצע בעזרת סימולציה התחברות ליחידות החסרות ויכין את המערכת שלו לקליטה עתידית של היחידות שטרם חוברו. לנושא זה תהיה קבלה נפרדת.

7.1.5.3 במידה ובמשך תקופת ההרצה/תקופת האחריות ניתן יהיה לחבר את המערכות החסרות, הקבלן יחברן ללא כל תוספת מחיר, במסגרת חובותיו בתקופת האחריות.

7.1.5.4 סיום העבודה בנוסף לכך יהיה לאחר קבלתה, הרצה והדרכה כמפורט במפרט זה.

7.1.6 תיעוד

7.1.6.1 עם מסירת המערכת לידי המפקח יגיש הקבלן 3 עותקים בעברית של תיעוד המערכות האלקטרוניות וציוד הבידוק .

7.1.6.2 תיעוד זה יכלול:

7.1.6.2.1 תאור המערכת ועקרון פעולתה (כולל ספציפיקציות טכניות).

7.1.6.2.2 הוראות הפעלה ותחזוקה בדרג א - מפעיל (הוראות מפורטות, תרשימי זרימה, בליווי הסבר בשרטוטים על פקדים וכו', כולל צילום צבעוני של כל מרכיבי הציוד במיקומם הסופי, הצילום יבוצע בתאום עם המתכנן/מזמין).

7.1.6.2.3 הוראות הפעלה מקוריות של היצרנים השונים.

7.1.6.2.4 הוראות אחזקה מונעת, איתור ותיקון תקלות מפורטות לכל תת מערכת. כולל רשימת חלקי חלוף מומלצים (מספרים קטלוגיים שם וכתובת היצרן לכל פריט).

7.1.6.2.5 תוכניות AS-MADE.

7.1.6.3 עם גמר העבודות, יכין הקבלן לפי תכניות הביצוע, מערכת התכניות של כל העבודות ושל המתקנים והמערכות, עליהן יסמן וישרטט בפרוטרוט את העבודות שבוצעו למעשה ואת חלקי המתקנים כפי שהוצבו סופית. כל הפרטים שיסמן הקבלן בתכניות הנ"ל יהיו טעונים בדיקה ואישור המתכנן והמפקח.

7.1.6.4 לשם הכנת תכניות אלו ע"י הקבלן יספק המתכנן למפקח, לפי דרישת הקבלן, את התוכניות הנדרשות, עליהם יסמן הקבלן את העבודות הנ"ל. הקבלן ישמור על כל תכנית שנוי ותיקון שייעשו תוך כדי ביצוע העבודה. התכניות כפי שבוצעו בצרוף תכניות שינוי ותיקון ימסרו ב- 5 העתקים בתיק פלסטי קשיח למפקח לפני ביצוע התשלום הסופי. עבור הכנת התכניות הנ"ל לא ישולם בנפרד ותמורתו כלולה במחירי היחידה.

7.1.6.5 תוכניות מכניות ואלקטרוניות.

7.1.6.6 תוכניות חיווט.

7.1.6.7 פרוספקטים טכניים של ציוד שהותקן במערכת מסופררים בהתאם לסדר הופעתם בספרות התפעולית והטכנית.

7.1.6.8 נוהלי בדיקה ברמת המפעיל וברמת הדרג הטכני. כולל התייחסות מיוחדת לתקופת ההרצה. ונהלים אלו יכתבו כתרשימי זרימה.

7.1.6.9 רשימת חלקים וחלפים מומלצים לאחזקת המערכת. במידה והמזמין יבצע את התחזוקה לבדו.

7.1.6.10 רשימת כלי עבודה וצב"ד ייעודי הדרוש לאחזקת המערכת.

7.1.6.11 כתיבת הספרות תעשה בתאום מלא עם המזמין, לאחר גמר הכנת הספרות יעביר הקבלן למתכנן לפני מסירת המערכת טיוטה לאישור. לאחר קבלת הערות המפקח יסיים הקבלן את הכנת ספרות המערכת.

7.1.6.12 בנוסף לחומר הכתוב שיוגש נדרש הקבלן למסור העתק במדיה מגנטית כדיסק מלל ב-WORD ושרטוטים ב AutoCad.

7.1.6.13 העמדת מחשב נייד מתקדם ביותר למועד מסירת המערכת, לטובת טיפול ועדכוני תוכנה אשר ישמש את טכנאי השרות לעבודה באתר, המחשב יישאר באתר וייעמר אצל קב"ט האתר, ע"ג המחשב יותקנו כלל התוכנות הנדרשות לעבודה על המערכת וכן תיקי התיעוד של המערכת כולל כלל השרטוטים של המערכת והאתר . טכנאי השירות

לא יורשו לעבוד על המערכת עם מחשבים ניידים אחרים וכל עדכוני התוכנה וטיפול במערכות יבוצע עם מחשב זה בלבד.

כמו כן יודגש כי כלל העדכונים של התוכנות לא יבוצעו אונליין וכל עדכון תוכנה יבוצע באמצעות דיסק , חיבור של רכיב אלקטרוני למערכת יבוצע אך ורק לאחר העברת הרכיב בעמדת הלבנה ולאחר אישור של הממונה על אבטחת המידע באתר ובחברה.

7.1.6.14 ספרות המערכת תימסר ביום מסירת המערכת לידי המפקח.

7.1.6.15 קבלת המערכת מהקבלן מותנית בין היתר בביצוע של פרק זה.

7.1.7 הדרכה

7.1.7.1 הקבלן יקיים על חשבונו הדרכה, 5 ימים לפחות לפני מסירת המערכת למזמין. ההדרכה תהיה עיונית ומעשית מסודרת למפעילים של המזמין, כדי להכשירם לביצוע פעילויות תפעול של המערכת.

7.1.7.2 הקבלן יבצע את כל פעילות העזר הדרושה לצורך העברת השתלמויות, כולל הכנת ספרות הדרכה שתאושר ע״י המזמין. ספרות זו תהווה חלק/פרק בספרות התיעוד.

7.1.7.3 ההדרכה הנ״ל תהיה במסגרת של 6 שעות לפחות ותתקיים באתר ב – 2 מועדים שונים שיקבעו ע״י המזמין עם הקבלן.

7.1.7.4 בנוסף תבוצע הדרכה מיוחדת לרמת מנהלים/קב״טים. הדרכה זו בת 2 שעות לפחות תבוצע ב - 2 מועדים שונים שיקבעו ע״י המזמין עם הקבלן.

7.1.8 אחריות בתקופת הבדק

7.1.8.1 בכל מקום במפרט בו מצוין תקופת אחריות הכוונה לתקופת הבדק.

7.1.8.2 הקבלן יהיה אחראי כלפי המזמין כי הציוד או המערכת המסופקת על ידו, האביזרים והחלפים יפעלו בתקינות ויעמדו בבצועים הנדרשים בהתאם למפרט הטכני ולתנאי המסמך ויהיו חופשיים מכל פגם בחומר, עבודה או בתכנון. הקבלן אחראי שהציוד/המערכת או המערכות והמכשירים השונים יעבדו בצורה תקינה ומשולבת בכל הקונפיגורציות הנדרשות עם מערכות אחרות ובינם לבין עצמם כמפורט במפרט הטכני המיוחד.

7.1.8.3 הקבלן יהיה אחראי לכל מגרעת, לקוי, פגם או קלקול שיתגלה בביצועי

המערכת, הציוד או תת-המערכות, באביזרים או בחלפים הנובעים מעבודה גרועה ו/או עקב שימוש בחומרים, מכשירים, חלקים וציוד פגומים ו/או שאינם מתאימים לאפיון הטכני ו/או הנובעים מתכנון לקוי.

7.1.8.4 תקופת האחריות/בדק הנה 24 חודשים שתחילתם בתום הקבלה הסופית בהצלחה של כל המערכות.

7.1.8.5 במהלך תקופת האחריות הקבלן מתחייב לתקן או להחליף בחדש כל ציוד ו/או חלקים אשר ימצאו לקויים, פגומים או בלתי תקינים תוך שימוש במערכת, בציוד ו/או בחלפים. אם תוקן חלק פגום, או לקוי, שלש פעמים ע"י הקבלן, יחויב הקבלן להחליפו בחלק חדש ולא יורשה לתקנו עוד.

7.1.8.6 התיקון יבוצע באתר בו מופעל, מותקן, או מאוחסן הפריט הלקוי.

7.1.8.7 תיקן הקבלן ו/או החליף במסגרת התחייבויותיו חלק לקוי או פגום - יחול מנין תקופת האחריות על החלק המוחלף או המתוקן, מיום בצוע התיקון או ההחלפה מקסימום שנה לאחר סיום העבודה.

7.1.8.8 בתקופת האחריות מתחייב הקבלן לבצע במערכת את כל השינויים הנדרשים אם יתברר כי פעולת המערכת או הציוד לקויים עקב השפעת המכשירים ותת המערכות השונות שנכללו במערכת.

7.1.8.9 תיקון ו/או החלפה לצורך סעיף זה פירושו : איתור התקלה, קבלת אישור המפקח לשנוי בציוד/מערכת, הובלה, התקנה, חבור, החלפת רכיבים, שינוי טכני, כוונון בדיקה, וכל פעולה אחרת שיעודה להביא את המערכת לפעולה תקינה ולהעמידה בבצועים הנדרשים בהתאם למפרט הטכני.

7.1.8.10 הקבלן ישא על חשבונו בכל ההוצאות הכרוכות בביצוע התיקון ו/או ההחלפה במתכונת שהובהרה לעיל, פרט לבלאי שוטף במצברים החל מהשנה השלישית לחיי המערכת.

7.1.8.11 הקבלן יבצע תחזוקה מונעת בביקורים מתואמים פעמיים במשך השנה הכוללת :

7.1.8.11.1 בדיקה חזותית לתקינות הציוד, חווט, שילוט.

7.1.8.11.2 הפעלה מלאה של כל המערכות והציוד ובדיקת פעולה של כל הפונקציות.

7.1.8.11.3 בדיקת עבודה במתח מצברים ובדיקת תקינות כל מקורות המתח.

7.1.8.11.4 בדיקת התקנת הציוד במסדים, ארונות IDF, MDF, שולחנות בקרה ותשתיות.

7.1.8.11.5 בדיקה לפעולה תקינה, בכל רמות התפעול הנדרשות, וברמות התפוקה החשמליות והאלקטרוניות הנדרשות מציוד מותקן ומתופעל.

7.1.8.11.6 בדיקת הארקה והגנות ברקים.

7.1.8.11.7 בדיקת שלמות פיזית של הציוד והתשתיות (כבלים), הכוללת בדיקת חלודה, צבע, ומפגעים אחרים.

7.1.9 דו"חות

7.1.9.1 הקבלן נדרש להגיש דוח עבור כל תיקון ובדיקה תקופתית שיבצע, הדו"ח יכלול :

7.1.9.1.1 שם מזמין השרות.

7.1.9.1.2 זמן קריאה, זמן הגעה לשטח, זמן סיום הטיפול.

7.1.9.1.3 תאור התקלה.

7.1.9.1.4 תאור התיקון שבוצע.

7.1.9.1.5 פירוט רכיבים, מכלולים, יחידות שהוחלפו/תוקנו.

7.1.9.1.6 כל דו"ח יימסר ב- 2 העתקים.

7.1.9.1.7 כל דו"ח ייחתם ע"י נציג המזמין והקבלן המבצע.

7.1.9.2 כל הרשום בדוחות, יוזן וינוהל במאגר ממוחשב, באחריות הקבלן, בתוכנת ניהול תחזוקת מערכות ורכיבים אלקטרונים.

7.1.9.3 החלפים המינימליים שיחזיק הקבלן יהיו ברמה של מכלולי המערכת, וכן רכיבים בתוך המכלולים. רשימת החלפים תיבנה על-סמך טבלאות שיוכנו ע"י הקבלן ויאושרו ע"י המתכנן. כמות חלפים - כמות מלאי החלפים תחושב התאם לכללים הבאים :

7.1.9.4 כמות של 5% מהיקף המערכות.

7.1.9.5 מינימום 2 יחידות מכל סוג.

7.1.9.6 החברה תתחייב, במסגרת האחריות ועל חשבונה, לטפל בפגמים טכניים או פונקציונליים חוזרים שיתגלו במערכת. הטיפול יכלול איתור מקור הפגם, מציאת פתרון טכני לפגם וביצוע הפתרון לכל המרכיבים הפגומים במערכת. החברה תתחייב לבצע בתקופת האחריות תיקון ואחזקה של המערכת בהתאם למפורט להלן :

7.1.9.7 אחזקה ותיקון של ציוד נישא יתבצעו במעבדות השרות של החברה. הציוד יימסר ע"י נציגי המזמין ללא תאום מוקדם.

7.1.9.8 תיקון האלמנטים יתבצע תוך 3 ימי עבודה.

7.1.9.9 הציוד המתוקן יוחזר כשהוא מלווה בתיעוד המגדיר התקלה והתיקון שבוצע.

7.1.9.10 תחזוקת תשתית המערכת תתבצע באתר בהתאם לקריאה של המזמין.

7.1.9.11 הגעה לאתר התקלה תוך 12 שעות מקבלת הודעה על תקלה כל שהיא ו - 4 שעות עבור קריאה במצב של תקלה משביתה (תקלה בה למעלה מ 50% של ההיקף ו/או המוקד אינם מתפקדים) בחברה בכל ימות השנה, זמן מרבי להשמשת המערכת הנה 6 שעות.

7.1.10 ליקויים חוזרים:

7.1.10.1 ליקויים החוזרים יותר מפעם אחת ואשר יקרו בתקופת האחריות תוך שימוש רגיל, והנובעים מחמת ביצוע לקוי, יתוקנו על ידי הקבלן ועל חשבונו באופן יסודי עד הבאת האתר למצב עבודה תקין.

7.1.10.2 ליקויים כנ"ל הנובעים מחמת חומר/ציוד פגום יוחלפו על ידי הקבלן ועל חשבונו בחדשים, תקינים.

7.1.10.3 האחריות על החלקים או עבודות בהם נתגלו ליקויים חוזרים, תתחיל מחדש מיום פעולה תקינה של החלק למשך 24 חודשים.

7.1.11 חוזה אחזקה ושירות לאחר תקופת האחריות (לאחר תקופת הבדק):

7.1.11.1 עם תום תקופת הבדק/האחריות מתחייב הקבלן להעניק למזמין שירות לתחזוקת המערכת לרבות אספקת חלקי חילוף למערכת וביצוע עבודות אחזקה שנתיות על מנת שהמערכת תמשיך לתת מענה לאורך כל שנות תקופת האחריות כפי שמפורטים בסעיף זה :

7.1.11.2 תקופת השרות : 10 שנים מסיום תקופת הבדק.

7.1.11.3 תנאי תקופת השרות האופציונלית יהיו זהים (לרבות זמן התגובה לקריאות) לתנאי מתן השירות בתקופת האחריות / הבדק.

7.1.11.4 הקבלן יצרף להצאתו מחיר לשעת עבודה באתר במקרה שתידרש עבודת טכנאי שאינה במסגרת הסכם השרות.

7.1.11.5 כוח עליון/שבר במזיד - תקלות שנובעות מכוח עליון או נזק במזיד יתוקנו ע"י הקבלן בהתאם לכל דרישות החוזה אולם התשלום עבור חלפים, מכלולים שיסופקו במקרה זה יתבצע עפ"י מחירי כתב הכמויות המקורי שהוגש במסגרת המכרז לביצוע המערכת כולל הצמדה.

7.1.11.6 יובהר כי מחירי המוצרים שמתמכר הקבלן בעת הצעת המחיר הראשונית להתקנת המערכות בבניין יהיו תקפים לאורך כלל ההתקשרות ולא יחולו מחירים שונים על מוצרים אלו.

7.1.11.7 בסיום תקופת השרות של ה-10 שנים יחליף היזם על חשבונו את כלל מערכת הביטחון במתקן במערכת חדשה שתותאם ברמתה הטכנולוגית למערכות הביטחון המותקנות במתקני הממשלה במועד ההחלפה.

הדבר רלוונטי לכלל מערכות הביטחון.

7.1.11.8 עם החלפת מערכות הביטחון יקבל עליהם היזם אחריות בהתאם לאמור לעיל עד לסיום תקופת האחריות שלו בבניין (21.5 שנים מעת חתימת הצדדים על חוזה התקשרות).

8 ההגנה בסייבר ורציפות תפקודית:

8.1 כללי

האיום בתחום הסייבר במרחב הקיברנטי הינו איום חדש יחסית הטופס מימד רחב ומשפיע על תחומים רבים מאוד, בין היתר גם על תחומי העשייה בהקמת מבנים בדגש על מבנים בעלי רגישות מתוקף היותם בנייני ממשלה בעלי חשיבות רבה לתפקוד הממשלה והמשך מתן שירותים גם במצב חירום וכן מתוקף ריבוי היחידות המאכלסות את המבנים והמידע הרגיש שקיים בהן.

8.2 מטרה

מטרת מסמך זה הינה הסדרת הדרישות בתחום ההגנה בסייבר לצמצום הנזק עד כמה שניתן מאירוע סייבר פנימי או חיצוני העלול להתרחש בעת הליכי הקמת המבנה שלא יבוצעו כנדרש והעלולות לשבש ו/או להשפיע על תפקוד היחידות והמשרדים המאכלסים את המבנה בשגרה ובחירום ומניעת דלף מידע הקיים במתקן בעקבות ביצוע מערכות ו/או תשתיות רגישות שלא כנדרש כמו כן במסגרת אכלוס המבנה ותפקודו קיימת רגישות רבה בייחס לתפעול המבנה ומערכותיו האלקטרומכאניות הקשורות לתפעולו השוטף של המתקן ויכולת של המשרדים המאכלסים לתפקד בוא הן בשגרה והן בחירום בהתאם לרמת השירות ויעדי השרות שהגדירו המשרדים המאכלסים את האתר.

8.3 האחריות והדרך למימוש ההנחיות

האחריות למימוש ההנחיות המוגדרות במסגרת מסמך זה יכולו על היזם .

לצורך כך יעמיד היזם יועץ בתחום ההגנה בסייבר בעל ניסיון בתחום זה מגופי הביטחון (צה״ל, שב״כ, משרד הביטחון) אשר עסק בתחום זה בשנתיים האחרונות לפחות וביצע פרויקטים בתחום ההגנה בסייבר עבור גופים אלו.

היועץ יציג את המענים והפתרונות לאישור מערך סייבר חירום וביטחון בכל תחום לפני תכנון מפורט/ יציאה לרכש ו/או ביצוע עבודות התקנת תשתיות ומערכות וכן יציג לאישור נציג מערך סייבר חירום וביטחון את הפתרונות שבוצעו באתר במהלך ביצוע העבודות וכן בסוף התהליך לצורך אישור כי אכן עמד היזם בכל ההנחיות וביצע אותן כנדרש.

יועץ היזם יכין תוכנית וספר מערכת לתחזוקה וניהול שוטף של האתר בייחס לתרחישי איום הייחוס שיוגדרו לו, ספר זה יהווה את הבסיס לניהול התחזוקה והשרות במתקן ויכלול מענה אפקטיבי שיאושר מראש לכלל התרחישים בחירום, ספר זה יוגש לאישור מערך סייבר חירום וביטחון לפני מסירת המתקן ולפני מעבר לשלב השירות על כל מערכותיו המעבר לשלב זה יהיה

בכפוף לאישור ספר זה שיחייב את כלל נותני השרותים במתקן.

8.4 הגדרת האיום

8.4.1 איום הסייבר מאופיין בהתאם לגורם העומד מאחורי האיום ואכן כפי שחווינו ממספר אירועי סייבר במהלך השנים האחרונות ניתן לחלק אירועים אלו בחלוקה הבאה :

גורמים חיצונים :

8.4.1.1 איום מעצמתי – (איום הנובע מהחלטה של מעצמה לפעול במרחב הקיברנטי)

8.4.1.2 איום מדינתי – (איום הנובע מהחלטה של מדינה לפעול במרחב הקיברנטי)

8.4.1.3 איום של ארגון טרור – איום הנובע מהחלטה של ארגון טרור לפעול במרחב הקיברנטי)

8.4.1.4 התארגנות אזרחית תעשיות וארגונים ציבוריים- (תקיפה באמצעות רשתות חברתיות)

8.4.1.5 אנשים בודדים (האקרים)

גורמים פנימיים :

8.4.1.6 עובד ארגון - (ממורמר ו/או מופעל)

8.4.1.7 סקרנים או עובדים שאינם מודעים לנושא אבטחת מידע

8.4.1.8 נותן שירות חיצוני - (טכנאי, ספק, זכיין וכו')

8.5 תחולת האיום

8.5.1.1 האיום הקיברנטי הינו איום רחב ביותר אשר במסגרתו יכול הגורם המאיים לפעול במספר אופנים בין היתר :

8.5.1.2 חדירה למערכות המידע .

8.5.1.3 איסוף מידע מבסיסי נתונים.

8.5.1.4 פגיעה בתשתיות פיסיות של התקשורת.

8.5.1.5 השבתת מערכות .

8.5.1.6 שינוי הגדרות תפעול במערכות.

8.5.1.7 התחזות.

8.5.1.8 הפלת מערכות .

8.5.1.9 הפלת התקשורת.

8.5.1.10 השתלטות.

8.6 המענה

8.6.1 המענה לאיום בתחום הסייבר כולל שילוב של מעגלי אבטחה רבים והתייחסות ספציפית לכל תהליך, במסגרת הקמת מבנה חדש, קיימים תהליכים קריטיים בהם חייבת להיות התייחסות ומעורבות של גורמי הביטחון הן בשלב ההגדרות הן בשלב הביצוע וכלה בשלב הקבלה והתפעול השותף.

8.6.2 במסמך זה נרכז את עיקרי ההנחיות ליזם על מנת שיוכל לתכנן את תהליכי הביצוע השונים החל משלב הדרישות לקבלני הביצוע דרך הליכי הרכש וכלה בתהליכי ההתקנה והתפעול של המערכות השונות במתקן.

8.6.3 אדגיש כאן כי עיקרי דרישות אלו הינן כלליות ואינן מפורטות עד השלב האחרון בכל תהליך, יועץ היזם במסגרת היערכותו למתן מענה יכין תוכנית מפורטת שתכלול את כלל הפעולות הנדרשות לביצוע על ידי היזם והקבלנים המבצעים על מנת שהיזם יעמוד ביעדים להגנה כפי שנקבעו על ידי המזמין.

8.7 פירוט הדרישות

במסגרת פעולות היזם עליו לתת מענה לכלל הדרישות המפורטות מטה באמצעות יועץ ההגנה בסייבר אשר יכין מסמכים לאישור המזמין הכוללים נספחים שיוגדרו לביצוע על ידי נותני השירותים השונים בפרויקט הנספח יכלול את הסעיפים/מוספים בתחומים הבאים :

8.7.1 רציפות תפקודית והמשכיות עסקית בחרום.

8.7.2 אבטחה פיסית וביטחון.

8.7.3 סיווג עובדים.

8.7.4 אבטחת מידע וסיבר.

8.7.5 סעיף/מוסף רציפות תפקודית והמשכיות עסקית בחרום:

8.7.5.1 סעיף/מוסף זה יגדיר את כל הדרישות בתחום הרציפות התפקודית וההמשכיות העסקית של השרות/המוצר בו עוסק המכרז/הספק בחרום, ויכלול בין היתר את הנושאים הבאים :

8.7.5.2 אמצעי גיבוי ויתירות כאשר השרות/המוצר הראשי המסופק מושבת (יתירות מערכות/גיבויי מתח/גיבוי גנרטור/גיבוי אל פסק/ גיבוי תקשורת/גיבוי מיזוג אוויר/TIRE וכדי).

8.7.5.3 הגדרת משך הזמן שבו ניתן לספק את המוצר בשעת חרום ללא תלות בגורמים חיצוניים/אחרים (לדוגמא : כמות דלק בגנרטור המספיקה ל-3 ימי עבודה רצופה).

8.7.5.4 אספקת השרות/המוצר בשעת חרום-התחייבות הספק או מתן מענה אחר ע"ח הספק .

8.7.5.5 הגדרות בנוגע למיקום בו יסופק השרות (בהיבט שרידותו בחרום-עילי/תת קרקעי, אזור גאוגרפי וכדי).

8.7.5.6 רמת הזמינות של השרות המסופק.

8.7.5.7 תיעוד של המוצר/השרות (As Made) ובקרת תצורה על מערכות.

8.7.5.8 רמת השרות הנדרשת ברגיעה ובשעת חרום (SLA) :

8.7.5.9 כולל זמן הנדרש לתחילת עבודה על תקלה מרגע ההודעה .

8.7.5.10 כולל משך הזמן מרגע ההודעה ועד למתן מענה חלופי/תיקון התקלה.

8.7.5.11 אופן הניטור, ההתרעה והדיווח על תקלות בשרות/במוצר.

8.7.5.12 הצורך בהפעלת מוקד בקרה של הספק-וזמני פעילותו הנדרשים.

8.7.5.13 אישור מפעל חיוני של הספק (במידה והשרות/מוצר חיוני בשע"ח).

8.7.5.14 תשתיות לעבודה בחרום-מרחב מוגן, מערכות סינון וכדי.

8.7.5.15 רמת המיגון הנדרשת של המוצר, המבנה שבו מסופק המוצר והמערכות התומכות בפעילותו (כולל אישור פקע"ר) :

8.7.5.16 מיגון כנגד פגיעה ישירה של רקטות בהתאם לאיום הייחוס שהוגדר לפרוייקט

8.7.5.17 מיגון כנגד פגיעה של טילים במרחק כפי שהוגדר לפרוייקט .

8.7.5.18 מיגון כנגד חל"כ/חלב"ג-למשך שעה.

8.7.5.19 מיגון כנגד רעידת אדמה הצפויה באזור.

8.7.5.20 מערכות הבטיחות שנדרשות ע"מ לתמוך באירועי בטיחות (בקרת מבנה, גילוי אש ועשן, כיבוי אש, מערכות הצפה, מערכות התרעה וכדי).

8.7.5.21 מערכת השו"ב :

8.7.5.22 תכנון המאפשר הערכות לאפשרות של פגיעה והמשך תפקוד במוד מופחת ובמוד "ידני".

8.7.5.23 יכולת בידול והפרדה.

8.7.5.24 הדרכה ותרגול- מהם ההדרכות והתרגולים שבהם יידרש הספק לעמוד ומהי תדירותם ע"מ לוודא שהשרות/מוצר מסופק בהתאם לדרישות בשעת חרום.

8.7.6 סעיף/מוסף אבטחה פיסית וביטחון

8.7.6.1 סעיף/מוסף זה יגדיר ויפרט את דרישות האבטחה הפיסית של המוצר/השרות המסופק ויעסוק בנושאים הר״מ :

8.7.6.2 אבטחה אנושית (רמת המאבטחים וכשירותם, חימוש המאבטחים, מספר המאבטחים בכל נק׳ זמן על חשבון מי יבוצע).

8.7.6.3 המיגון- המיגון הפיסי בהיבט האבטחתי (מיגון כנגד פריצה, ירי נק״ל, מטענים נישאים, חבלה בציוד היקפי ותשתיות).

8.7.6.4 אבטחה אלקטרונית (טמ״ס, מערכות הקלטה, מערכת בקרות כניסה, גלאי נפח/תנועה וכד׳).

8.7.6.5 הגדרת מוקד אבטחה המפקח על קיום האבטחה.

8.7.6.6 דרכים למניעת גישה לגורמים שאינם מורשים.

8.7.6.7 אופן ההתרעה על גישה של גורמים לא מורשים לשרות/למוצר.

8.7.6.8 מנגנוני תאום אספקת השרות עם קב״ט של מזמין השרות/המוצר.

8.7.6.9 ליווי ספקי השרות במתחמי המזמין.

8.7.6.10 הנחיות הביטחון במתקני מזמין השרות/המוצר (בהתאם לרמת הסיווג והנחיות קב״ט המתקן).

8.7.6.11 דרישה להתממת הרכש - למניעת פרסום רכש המוצר הספציפי ויעודו.

8.7.6.12 סעיף/מוסף-סיווג עובדים

8.7.6.13 סעיף/מוסף זה יגדיר את רמת הסיווג הביטחוני הנדרשת מהספק/נותני השרות את אופן בדיקתם ויכלול בין היתר את הנושאים הבאים :

8.7.6.14 רמת הסיווג הביטחוני של נותני השרות מטעם הספק (ע״פ הנחיית מערך סייבר חירום וביטחון).

8.7.6.15 הדרישות בנושא בדיקות סיווג לעובדים/ קבלני המשנה /נותני השירותים- ביחידות מסווגות (ע״פ דרישת הקב״ט של הגוף המקבל את השרות).

8.7.6.16 התניית תחילת מתן השרות/המוצר-בעמידה בכל הדרישות הביטחוניות וקבלת אישור ביטחוני מתאים לכל הגורמים מטעם הספק.

8.7.6.17 בדיקת הביטחון תבוצע על חשבון מערך סייבר חירום וביטחון באוצר.

8.7.7 סעיף/מוסף-אבטחת מידע וסייבר

8.7.7.1 סעיף/מוסף זה יגדיר את דרישות אבטחת המידע מהספק/השירותים/המוצרים ואופן שמירת סודיות של מידע מסווג הנוגע למוצר/לשרות/למזמין ויכלול בין היתר את הנושאים הבאים :

8.7.7.2 רמת הסיווג של המכרז/דרישת הרכש.

8.7.7.3 רמת הסיווג הנדרשת מהספק.

8.7.7.4 הבטחת שמירת המידע הנוגע למזמין-אליו נחשף הספק/מי מטעמו (כולל הצהרת

שמירת סודיות).

8.7.7.5 מיקום המוצר במתחמי המזמין (במטרה לצמצם גישה של הספק למידע שאינו רלוונטי לשרות/למוצר המסופק על ידו).

8.7.7.6 אמצעי אבטחת המידע הנדרשים מהספק :

8.7.7.7 יישום כלים לניתור חיבורים לא חוקיים.

8.7.7.8 הצבעה על אנומליות.

8.7.7.9 יכולת בקרה והלבנה של הכנסת עדכוני תוכנה וכל תוכן אחר למערכת.

8.7.7.10 הקשחת המוצר-צמצום האפשרות להתחבר ו/או להטמין פוגעניים או אמצעים העלולים לפגוע במוצר/בציוד.

8.7.7.11 מערכת סגורה-דרישה למערכת פנימית מנותקת מתקשורת חיצונית, ללא מרכיבים אלחוטיים, ללא אחזקה מרחוק.

8.7.7.12 דרישות להפרדת תשתיות תקשורת (בהתאם לסיווג המידע המועבר והנחיות רא"מ).

8.7.7.13 מגבלות בנוגע למערכות ניטור מרחוק.

8.7.7.14 הגדרת אמצעי הסתרה של המוצר/ השרות.

8.7.7.15 דרכי הגנה על מערכות העיקריות המבנה (גנרטורים, מיזוג, מערכות גילוי וכיבוי אש מערכות דלק, שסתומים ומגופים הנשלטים מרחוק , מערכות שליטה ובקרה אבטחה ותקשורת).

8.7.7.16 מערכת השו"ב :

8.7.7.17 בקרת גישה למערכת (כרטיס חכם/קורא ביומטרי).

8.7.7.18 ניהול הרשאות והזדהות.

8.7.7.19 זכות המזמין לבקר במתקן היצור של הספק ולהכיר את נוהלי האבטחה הפיסית ואבטחת המידע של המוצר/ השרות.

8.7.7.20 במקרה של הפסקת שרות -אחריות הספק להעביר לנציג מערך סייבר חירום וביטחון כל רכיב בעל תכונות אגירת מידע (ללא תמורה) בהתאם לדרישות הגוף הביטחוני.

8.7.7.21 אחריות הספק שלא לבצע כל שימוש בהתקשרות עם גוף ביטחוני ללא אישור הגוף הביטחוני.

8.7.7.22 הגדרת נספח דרישות ביטחון ואבטחת מידע שיצורף להזמנת עבודה שתונפק ע"י גוף ביטחוני.

8.7.7.23 יצירת מערכת בקרה ממוחשבת לניהול ולגיבוש תהליכי תפעול ואחזקה :

8.7.7.23.1 על היזם לתכנן ולהקים עמדת בקרה לכל נושא ההגנה בסייבר וביטחון באוצר הממוקם בבניין הג'נרי בי-ם ותהווה עמדת S.O.C שתתופעל על ידי מוקד הביטחון, עמדה זו תרכז את כלל עמדה זו תוצב במוקד הבקרה הארצי של מערך סייבר חירום

ההתראות ברשת ותבצע ניתור ע״ב כלי ניתור סטנדרטיים – באחריות היזם באמצעות זכיין מערכות המנ״מ העברת המידע על גבי רשת מאובטחת IPVPN שתוגדר על ידי מערך סייבר חירום וביטחון למוקד הארצי.

8.7.7.23.2 מערכת זו תבוסס על תפיסת הגנה מתקדמת לזיהוי פעולות ברשת, המערכת תעבוד כמערכת הגנה דינאמית .

8.7.7.23.3 מערכת זו במסגרת תפקידיה תבצע ניתור של כלל הרכיבים המבוקרים במתקן ותתריע על כל פעילות חריגה ולא תקינה של מי מהבקרים ו/או נקודות הקצה.

8.7.7.23.4 כמו כן מערכת זו תתריע על כל פעולה חריגה על גבי תשתיות התקשורת בבניין ותציג את הפעולה החריגה על גבי מסך התרעות הכולל את איתור הנקודה המדוייקת בא אירע האירוע החריג סוג האירוע שעת האירוע וכו׳ .

8.7.7.23.5 באחריות היזם באמצעות ספק מערכות הביטחון חיבור והעברת מידע הכוללvideo ברמת איכות גבוה וכן מידע התראתי ברמת השו״ב לשו״ב העל PCM המוצב במוקד הארצי של מערך סייבר חירום וביטחון באוצר התשלום בגין עלויות הקו יושתו על עלויות התקשורת השוטפות של המתקן ההגנה על התשתית תוגדר לספק הזוכה בצד החיבור שבאחריותו (קרי בצד האתר) לאחר זכיתו בביצוע ולפני החיבור הסופי בהתאם להנחיות הגורם המקצועי במערך סייבר חירום וביטחון העברת המידע תהיה חד כיוונית מהמתקן למוקד הארצי ולא תתאפשר העברת מידע לתוך מערכות האתר .

8.7.7.23.6 מערכת לניטור שינוי ברכיבי הקצה (סייבר סוויץ׳) שתתוקן על כל רכיבי הקצה של מערכות הביטחון ותתריע על כל אירוע או שינוי ברכיב המקושר לרשת.

8.7.8 סעיף /מוסף אבטחה פיסית וביטחון במהלך ביצוע העבודות:

8.7.8.1 יצורף נספח הנחיות לביצוע עבודות באזורים רגישים בהתאם לתכנון בפועל וסיום תכנון עקרוני .

8.7.8.2 נספח זה הינו חלק מדרישות ההגנה בסייבר ועל היזם לבצע את העבודות בהתאם לדרישות אלו.

8.7.8.3 היזם יתמחר עלות זו בנפרד ויציג את עלות הליווי הנדרש באמצעות עובדים שיאושרו לכך על ידי קב״ט היזם וקב״ט המזמין.

9 אחריות

10.1 נציג מערך סייבר חרום וביטחון :

10.1.1 אפיון איום הייחוס למתקן והמענה הנדרש.

10.1.2 השתתפות בדיוני התנעת מכרזים/תהליכי רכש הרלוונטיים לתחומי העיסוק של מערך סיבר חרום וביטחון.

10.1.3 אישור נספח סייבר חרום וביטחון להתקשרויות רלוונטיות של היזם.

10.2. אחריות היזם :

10.2.1 אחריות היזם שיתוף יועץ הסייבר בהכנת המכרזים וההתקשרויות.

10.2.2 עמידה בכל דרישות מסמך זה במהלך ביצוע הפרויקט.

10.2.3 מתן מענה בהכשרה הדרכה ביקורת ותרגול במהלך תקופת האחריות והשירות של המערכות.

10.2.4 התאמת תוכנות ושדרוג מערכות אשר נמצאו כבלתי יעילות או חדירות לאורך זמן ההתקשרות ותקופת מתן השירותים לתחזוקה בהתאם לחוזה התחזוקה .

10 תיעוד ופעולות נוספות במסגרת תקופת השירות:

11.1 באחריות היזם עם ביצוע המסירה להעמיד למזמין את המסמכים הבאים במדיה מגנטית ובשלשה עותקים מודפסים .

9.2. הכנת תוכנית מסירות :

9.2.1. באחריות יועץ היזם הכנת תוכנית מסירות לבחינת ביצוע דרישות האבטחה ATP .

9.3. הכנת תוכנית הכשרה למפעילים :

9.3.1. באחריות היזם הכנת מסמכי הדרכה והכשרה באמצעות כל גורם חיצוני אחר אשר סיפק ציוד ו/או מערכות למתקן.

9.4. הכנת תוכנית בקרה וביקורת :

9.4.1. באחריות היזם להכין תוכנית בקרה וביקורת בהתאם להנחיות ספקי הציוד והאמצעים ו/או לחילופין בהתאם להנחיות הגורמים המקצועיים הרלוונטיים.

9.5. הכנת תוכנית פיקוח ותרגול :

9.5.1. באחריות היזם הכנת תוכנית לביצוע ביקורות לפיקוח על תקינות המערכות באופן שוטף וכן על בחינת הידע אצל הגורם המתפעל של הציוד והמערכות השונות במתקן, כום כן באחריות היזם לבצע הכשרות ותרגילים למערך התמך הלוגיסטי הכולל את אנשי התחזוקה והניהול של המתקן מערך האבטחה על כל רכיביו .

9.6. איתור תהליכים מסכנים בתחום הסייבר ומתן התראה למזמין על הסיכון :

9.6.1. באחריות היזם ו/או יועציו בכל התחומים להתריע בפני המזמין על כל איום נוסף אשר קיים במערכותיו ו/או אשר עולה במהלך התקופה גם לאחר ההתקנה וזאת לאורך כל תקופת השירות על הציוד והמערכות המותקנות באתר.

9.7. יצירת תיק נהלים ליישום ההגנה במערכות :

9.7.1. באחריות היזם באמצעות החברות והיועצים להכין תיק נהלים והנחיות לתפעול שוטף של כלל הציוד המותקן באתר וכן לעדכן תיק הנחיות ונהלים זה אחת לשנה לפחות ובכל פעם בו עולה צורך לעדכון .

9.7.2. היזם יכין פרק תפעול בחירום של כלל האמצעים והרכיבים הדרושים תפעול שונה בחירום בדגש על הפעלות ידניות הנדרשות להמשכיות ורציפות תפקודית של המתקן בחירום.

בברכה,

בנצי פיליפסון

ס.ראש מערך סייבר חירום וביטחון

העתק : מנהלת הקמת קריות הממשלה