מדיניות תחום האירוח

בממשל זמין

גרסה 1.0

מעקב גרסאות

מס"ד	תאריך	עודכן על ידי	תיאור השינויים
1.0	10.10.2016	אופיר יהב	גרסה ראשונה

נתוני גרסת המסמך

גורם	תפקיד	שם מלא	תאריך	חתימה
נערכה ע"י	PMO	אופיר יהב	28.9.2016	(חתימה)
נבדקה ע"י	מנהל תחום בדיקות אפליקציה	יוגב מזרחי	26.9.2016	(חתימה)
נבדקה ע"י	מנהל תחום פיתוח במערך ה-IT	עודד פוקס	9.10.2016	(חתימה)
אושרה ע"י	מנהל מערך סייבר ואבטחת המידע	אברהם זרוק	9.10.2016	(חתימה)

תוכן עניינים

1. כללי

1.1. מסמך זה מפרט את קווי המדיניות של ממשל זמין בתחום אירוח האתרים.

1.2. מטרת המסמך הינה להתוות את מדיניות ממשל זמין בכל הקשור לאירוח אתרים בתשתיות ממשל זמין – לאורך כל מחזור חיי האתרים – מאפיון האתר, הקמת התשתית לאירוח האתר, בניית האתר, בדיקתו, השקתו, עדכונו ותחזוקתו – תוך שמירה על כל כללי, הוראות והנחיות אבטחת המידע בכל שלב ושלב.

1.3. המסמך נכתב עבור עובדי ממשל זמין ועבור לקוחות ממשל זמין – משרדים, יחידות סמך וגופים ממשלתיים אחרים – המארחים את אתריהם בתשתיות ממשל זמין.

2. אחריות ליישום המדיניות

2.1. **מנהל מערך הגנה בסייבר** – קביעת מדיניות הגנה בסייבר ואבטחת המידע ובחינת היישום הנחיות המדיניות, הוראות אבטחת המידע כלליה ונהליה.

2.2. **מנהל מערך ה-IT** - קביעת מדיניות תחום האירוח ועדכונה מעת לעת. אחראי, אחריות ניהולית, על יישום המדיניות.

2.3. **מנהל תחום אירוח** – אחראי, תפעולית, על יישום המדיניות ודיווח למנהל מערך ה-IT אודות מידת היישום של קווי המדיניות או חריגה ממנה.

3. קווים מנחים לאירוח אתרים בממשל זמין

3.1. אירוח האתרים בממשל זמין יתבצע תוך יישום ההנחיות, ההוראות והכללים המפורטים במסמכים ובמקורות הבאים:

3.1.1. מדיניות הגנה בסייבר ואבטחת המידע

3.1.2. מדיניות פיתוח מערכת מאובטחת.

3.1.3. תקינה והסמכות אליהם מחויב ממשל זמין ובכללם תקן ISO-27001, הוראות ISO-27032, ISO-9001, תקן PCI-DSS.

3.1.4. חוק הגנת הפרטיות התשמ"א-1981 והוראות רמו"ט בנושא הגנת הפרטיות.

3.1.5. תקן Gov.IL למימוש תשתית צומת השירותים בממשל זמין.

3.1.6. נהלי ממשל זמין העוסקים בין היתר בתחומים הבאים:

3.1.6.1. הקמת ואירוח אתרים

3.1.6.2. תהליכים במערך ה-IT המהווים תשתית להקמת האתר.

3.1.6.3. הזדהות חכמה – תשתית זהות דיגיטלית וכרטיס חכם

3.1.6.4. התקשרות עם ספקים חיצוניים.

3.2. הקמת האתר תתבצע תוך שמירת העקרונות הבאים:

3.2.1. **התאמת תשתית האתר** (ובכללה החומרה) והטכנולוגיה המשמשת להקמת האתר לאופי האתר וייעודו.

3.2.2. **שרידות האתר** - במטרה לשמור על רציפות השירות ואיכותו תוך הקצאת המשאבים הנחוצים לכך.

3.2.3. **עקרונות הגנה בסייבר ואבטחת המידע** – אשר נועדו להבטיח את זמינות, שלמות וחסיון המידע המועבר באמצעות האתר – תוך שמירת כללי אבטחת המידע (כגון הפרדת רשתות, שימוש באתר טסט, בדיקות חוסן וכיו"ב) אשר נועדו להגן הן על האתר והן על שאר תשתיות ממשל זמין.

4. הקמת והשקת אתר

4.1. הקמת האתר תתבצע לאחר ביצוע אפיון מפורט, קיום DR (Design Review), ניתוח והערכת עומסים, כמו כן יש לבחון מול תחום אירוח היתכנות של כל אחד מרכיבי המערכת לפני הטמעת המערכת.

4.2. **תמיכה במערכות הפעלה ותוכנות צד ג'**

4.2.1. אירוח אתרים יהיה מבוסס על טכנולוגיות ותשתיות הנתמכות על ידי היצרניות - ושאינן End-Of-Life – ניתן לקבל פרטים נוספים בנספח הטכני למסמך המדיניות.

4.2.2. קיימת תמיכה במרבית מערכות ההפעלה המבוססות מבית מיקרוסופט ו Linux הנתמכות על ידי היצרן. מערכות ההפעלה צריכות להיות מעודכנות בצורה מלאה. תחום האירוח בממשל זמין מבצע עדכון של מערכת ההפעלה ועל הלקוח לדאוג לתאימות של האפליקציה מול העדכונים האחרונים.

4.2.3. קיימת תמיכה בבסיסי נתונים של החברות המוכרות בתחום ומאושרות בממשל זמין ובגרסאות אשר נתמכות על ידי היצרן.

4.2.4. קיימת תמיכה בשרתי ה – WEB המוכרים בתחום לרבות מיקרוסופט (IIS) ו – Apache.

4.2.5. קיימת תמיכה במערכות ניהול תוכן (CMS) של חברת מיקרוסופט בגרסאות עדכניות. כמו כן נתמכות גם מערכות ניהול תוכן של Drupal בתשתית הקוד

הפתוח. מערכות ניהול תוכן של צד ג' נתמכות בתנאי שהלקוח דואג לתמיכה למוצר על ידי גורם חיצוני לעבודה מול Tier -2 של תחום האירוח בממשל זמין. על מנת להשתמש במערכת ניהול צד ג', על הלקוח לאשר את המערכת מול גורמי הגנה בסייבר ואבטחת המידע של ממשל זמין.

4.2.6. קיימת תמיכה במוצרים מחברות צד ג', כאשר נדרש לאשר מול גורמי אבטחת המידע של ממשל זמין את המוצר ואופי התקנתו באתר האירוח. ממשל זמין שומר לעצמו את הזכות להזמין את היצרן של המוצר או נציגו ולתשאל אותו על המוצר ואופן פעולתו. הלקוח צריך לדאוג לתמיכה למוצר על ידי גורם חיצוני לעבודה מול Tier -2 של תחום האירוח בממשל זמין. ממשל זמין שומר לעצמו את הזכות לא לאשר טכנולוגיה או פתרון שאינם עומדים בדרישות הגנה בסייבר ואבטחת המידע.

4.2.7. שימוש בקוד ומוצרי צד ג' כמו plugin, מחלקות עזר, מוצרי משלימים וכו' דורש אישור מראש, בדיקות חדירות וסקר קוד.

4.3. תמיכה בטכנולוגיות פיתוח

4.3.1. ניתן להשתמש בטכנולוגיות פיתוח שונות לאתרים כגון ASP.NET, MVC. כל הפיתוח צריך להתבסס על מדיניות פיתוח מאובטח של ממשל זמין.

4.3.2. ייושמו בהקפדה כל עקרונות הפיתוח המאובטח במתודולוגיית SDL (Security development lifecycle).

4.3.3. בכל הקשור לצומת השירותים, כל שירותי הרשת יפותחו וייושמו על פי הוראות תקן Gov.IL עבור Web Services.

4.3.4. בנושא הזדהות לשרתי ה – Web:

4.3.4.1. בממשל זמין ישנם כמה סוגי אתרי אינטרנט:

- אתר אשר אינו דורש הזדהות מהצד של הלקוח (אתר אנונימי).
- אתר אשר דורש הזדהות אפליקטיבית כגון שם משתמש וסיסמה.
  - יש להיערך ליישום הזדהות באמצעות OTP כתנאי הכרחי לקבלת שירותים.
- אתר מזוהה, הנמצא מאחורי מערכת הזדהות של כרטיס חכם, המגביל את הגישה בהתבסס על הנתונים הנמצאים בכרטיס החכם. משתמש המנסה להגיע לאתר עם כרטיס חכם ואינו מורשה לא יוכל להגיע לאותו אתר.

4.3.4.2. קיימים היום שלושה סוגי כרטיסים חכמים שעובדים עם המערכת:

- כרטיס תמוז שמונפק לכל עובדי הממשלה על ידי ממשל זמין.
- כרטיס של חברת Comsign.

- כרטיס של חברת Personal-ID.

4.3.5. **שימוש ב- Iframe** - אין להשתמש ברכיב IFRAME בתוך הפתרון. אם יש צורך להציג מידע מאתר אחר הדבר יתבצע באמצעות פתיחת דף נפרד.

4.3.6. **מידע מאתר צד שלישי** - כל מקום באתר בו מוצג מידע מצד ג' יסומן בצורה ברורה עם כיתוב "*המידע המוצג מגיע מאתר X*".

4.4. **העלאת קבצים למערכות**

4.4.1. ממשל זמין מאפשר העלאת קבצים באמצעות מערכת File Upload ייעודית של ממשל זמין הניתנת להטמעה באתר.

4.5. **סקר קוד ובדיקות חדירות:**

4.5.1. מבדקי חדירות ובדיקות קוד הינם שלבים הכרחיים במחזור החיים של כל אתר ושירות רשת (Web Service). סריקות קוד ומבדקי החדירות מבוצעים לצורך איתור חולשות ופגיעויות אבטחה אפשריות.

4.5.2. אתרים המתארחים בממשל זמין נדרשים לקבל את אישור תחום בדיקות חדירות אפליקציה במערך הסייבר ואבטחת מידע לצורך עלייתם לאוויר.

4.5.3. העלאת אתר חדש תלווה במסמך גרסה (ייכתב על-ידי הלקוח) המתאר את כלל מרכיבי האתר. ממסמך זה יגזרו סוגי הבדיקות הנדרשות.

4.6. **חומת אש אפליקטיבית – WAF:**

4.6.1. מרבית האתרים המתארחים בממשל זמין מוגנים באמצעות חומת האש האפליקטיבית.

4.6.2. בסיום בדיקות החדירות, רגרסיה וכו', יועבר האתר אל מאחורי ה-WAF לצורך "למידתו" במשך כשבועיים, בניית פרופיל ונעילתו.

4.6.3. לאחר בניית הפרופיל ונעילתו, הלקוח יבצע בדיקות קבלה ואז ייקבע תאריך מבוקש לעליה לאוויר.

4.7. הטיפול בתקלות ייצור יתבצע על פי אמנת השירות המעודכנת של ממשל זמין ונוהל אירוע מסוג תקלה.

4.8. **כמענה לדרישות תקן ISO:**

4.8.1. יש לוודא כי באתר קיימת תצוגה של הודעות קצרות, המספקות סיכומים ברורים, תמציתיים בני עמוד אחד (תוך שימוש בשפה פשוטה) של המדיניות החיוניות של המשרד או יחידת הסמך – בעלי האתר - תוך מתן קישור בהודעה לדוחות משפטיים מלאים ומידע רלוונטי נוסף עבור המשתמש (ובין היתר תנאי שימוש).

4.8.2. האתרים המתארחים בממשל זמין צריכים להיות מוחצנים באופן המאפשר למשתמשים לאמת את נותן השירותים. לדוגמא, שמות המתחם של אתרים המתארחים בממשל זמין חייבים להיות בסיומת Gov.il כך שהמשתמש ידע שהוא פונה לאתר ממשלתי. על פי בקרה זו לא יתארחו בממשל זמין אתרים שאינם שייכים לגופי הממשלה ויחידות הסמך.

4.9. **נוהל קמפיין**

4.9.1. ניהול קמפיין יחייב את תחום אירוח להערך מראש ולהכין את האתר לעמידה בעומסים גבוהים המאפיינים את הקמפיין.

4.9.2. נוהל קמפיין מסדיר את הפעולות אשר צריכות להתבצע טרם עליית קמפיין לאוויר ובזמן הקמפיין – מעקב אחר ניצול משאבי האתר והקצאת משאבים נוספים במידת הצורך.

4.9.3. לקוח ממשל זמין (המארח אתר העומד בבסיסו של קמפיין) נדרש לתאם מראש את ניהול הקמפיין ולקבל את אישור ממשל זמין למוכנות האתר לקמפיין.

5. עדכון ותחזוקה של אתר

5.1. **עדכון תוכן האתר** בסביבת האירוח של ממשל זמין יתבצע אך ורק בסביבה אחורית באחת הדרכים הבאות:

5.1.1. מערכת ניהול התוכן של האתר המוגנת באמצעות תשתיות כרטיס חכם.

5.1.2. כאשר אין מערכת ניהול תוכן, אפשר לעדכן את תוכן האתר על ידי העברת קבצים מאובטחת (באמצעות מערך הכספות) לשרת המארח את האתר.

5.2. **עדכון גירסת האתר** - יתבצע בתיאום מראש על ידי עובדי תחום האירוח בהתבסס על נוהל העלאת גירסת אתר (קיים מסמך ללקוחות המפרט את תהליך זה).

5.3. עדכונים ושינויים לתוכנה/תשתית - כל שינוי במערכת (למעט עדכון תוכן) מהווה "גירסה" ועליו לעבור בדיקות חדירות וסקר קוד.

5.4. **גישה מרחוק לשרתים**

5.4.1. לא קיימת אפשרות של גישה מרוחקת ישירה לשרתים לרבות rdp או ssh או ftp.

5.4.2. גישה לרכיבי הפתרון ברמת מערכת ההפעלה/מערכת הקבצים - הגישה לשרתים תתבצע ממתקני ה-ISP עצמו. לא תתאפשר גישה מרוחקת לשרתים או לחלקי המערכת.

5.5. **DRP -Disaster Recovery Plan**

5.5.1. בימים אלו מוקם מערך DRP עבור תחום האירוח בממשל זמין, מערך ה – DR מוגדר כ – Active\Active ויוגדר פתרון לכל לקוח בנפרד על פי המערכת המותקנת באתר הייצור. על מנת להשתתף בפתרון ה – DR על הלקוח לעמוד בדרישות של ממשל זמין בנושא.

5.6. **וירטואליזציה**

5.6.1. על כל שרת תותקן חומת אש ומפרט החוקים המוגדר בו יועבר לממשל זמין (תחום האירוח ומערך הגנה בסייבר).

5.6.2. יש לדאוג להעברת מספרי הפורטים שבהם נעשה שימוש בשרת\ים לצורך הגדרה החוקים ברכיבי חומת האש.

5.6.3. מערך השרתים בתחום האירוח מבוסס רובו על תשתית וירטואלית. על הלקוח לבדוק תאימות לסביבה זו על פי צרכיו.

5.6.4. **תצורת מימוש** - הפתרון ימומש בתצורת Front/Back עם הפרדה מלאה לשלוש שכבות (Tier 3) - תצוגה, BL, מסד נתונים. אם נדרש רכיב ניהול הוא יבנה בנפרד בצד האחורי של המערכת.

5.7. Databases

5.7.1. תחום האירוח מתחזק ונותן אחריות מלאה ותמיכה על בסיסי הנתונים של הלקוחות.

5.7.2. ממשל זמין מתחזק סביבת SQL שיתופית אשר ניתן לארח בה בסיסי נתונים או לחילופין להתקין בסיס נתונים ייעודי על פי צרכי המערכת/האתר.

5.7.3. אירוח בסיסי הנתונים יהיה מבוסס על טכנולוגיות ותשתיות נתמכות על ידי היצרניות ושאינן End-Of-Life – לפרטים יש לקרוא בנספח הטכני למסמך המדיניות.

5.7.4. כל בסיס נתונים צריך לקבל את הסיווג הראוי לו על מנת להיות ממוקם בסביבה המיועדת לו.

5.7.5. במידה ונדרשת עבודה עם Reporting Service הגישה תתבצע לשרת ייעודי בפורט 80/443 בלבד.

5.8. ממשקים לשירותי ממשל זמין נוספים

5.8.1. **נאמן DNS ותפקידו** – על הלקוח יהיה למנות נאמן DNS אשר יהיה אחראי על שם המתחם של האתר. במינוי נאמן ה-DNS יהיה על הלקוח לקחת בחשבון כי אחריות זו חלה לאורך כל מחזור חיי האתר וכי נאמן ה-DNS יידרש לקחת חלק בפעולת שינוי שם האתר, או הסרתו מהרשת, גם שנים רבות לאחר השקת האתר.

5.8.2. **עדכון האתר** – עדכון האתר יתבצע בחדר מעדכנים הנמצא במתחמי ממשל זמין. על הלקוח יהיה לוודא את זמינות עמדת המעדכנים ולשריין את עמדת המעדכנים לשימושו, על פי צרכיו, ובשעות הפעילות שנקבעו לכך. כל מעדכן יהיה חייב בהצהרת התחייבות לשמירת סודיות והנחיות אבטחת המידע כתנאי לכניסתו למתחם ממשל זמין.

5.8.3. הוספת רכיבים לאתר קיים תתבצע על פי נוהל מפורט הקיים בנושא זה. הנוהל מפרט מהי רמת בדיקות אבטחת המידע הנדרשת על פי סוג ואופי הרכיבים המתווספים לאתר. כל שינוי/הוספה של רכיבים מחייב שיתוף צוות חדירות אפליקציה במערך הגנה בסייבר של ממשל זמין.

5.8.4. כל אתר המתארח בתשתיות ממשל זמין מחויב לעבור בדיקת חדירות ברמה הנקבעת על ידי מערך הגנה בסייבר בממשל זמין.

5.8.5. מבדקי חדירות ובדיקות קוד הינם שלבים הכרחיים במחזור החיים של כל אתר ושירות רשת (Web Service). סריקות קוד ומבדקי החדירות מבוצעים לצורך איתור חולשות ופגיעויות אפשריות. על מבדקים אלו להתבצע על פי סט כללים מוגדרים לביצוע בדיקות חוסן.

5.8.6. **בדיקות עומסים** – כל אתר אנונימי המתארח בממשל זמין מחויב בביצוע בדיקות עומסים ולעמוד בסטנדרטים אותם מציב ממשל זמין.

5.8.7. הוספה/שינוי רכיבים ילוו במסמך גרסה (על פי נוהל מפורט הקיים בנושא זה) המתאר את אופי השינוי. ממסמך זה יגזרו סוגי הבדיקות הנדרשות.

5.9. העלאת גרסה תתבצע במועד אשר יתואם עם תחום אירוח בממשל זמין.

5.10. כל אתר מחויב **בבדיקות חדירות חוזרות** כל 18 חודשים גם אם לא עבר שינויי גרסה או הוספת רכיבים.

5.11. **העברת לוגים משרתים** – ממשל זמין מאפשר קבלת לוגים מהשרתים על ידי תהליך אוטומטי (נדרש אפיון בנפרד) או על ידי פניה לצוות הבקרה.

5.12. **אפשרויות האירוח בממשל זמין**

5.12.1. בממשל זמין קיימות שתי אפשרויות להתארח ברשת האירוח:

- תשתית ייעודית עבור הלקוח, כלומר עבור הלקוח מוקצים שרתים ייעודיים (חוץ מה – DB), על מנת לארח את האתר ובתשתית זו לא מתארחים לקוחות אחרים.
- תשתית שיתופית בה מתארחים מספר אתרים של לקוחות שונים כגון חוות Share Point.

5.13. **סביבות עבודה**

ברשת האירוח של ממשל זמין יש שתי סביבות עבודה עבור האתרים. לא קיימות ברשת האירוח סביבות פיתוח וסביבות ניסוי עבור האתרים המתארחים בממשל זמין. הסביבות הקיימות הן:

5.13.1. **סביבת ייצור** – סביבה זו חשופה ללקוחות ומנוהלת ברגישות גבוהה -על מנת לשמור על רציפות השירות ועמידה ב-SLA המוגדר באמנת השירות.

5.13.2. **סביבת .טסט/ Pre-Prod /STAGE** - סביבה נפרדת זו אינה חשופה לעולם, אלא אך ורק ללקוח. סביבה זו נועדה לביצוע בדיקות לפני שדרוג תשתית האתר או האתר עצמו ולבדיקות קבלה של הלקוח לאחר עדכון גרסה.

5.14. **תפעול מערכות ההפעלה של השרתים המארחים**

5.14.1. תחום האירוח בממשל זמין אחראי על התפעול השוטף של מערכות ההפעלה והאתרים של הלקוח. שירות זה כולל טיפול בתקלות, שינויי הגדרות ברמת השרת ותשתית האתר, הקמת השרתים והקשחתם.

5.14.2. כחלק ממערך השירות של ממשל זמין, כאשר מתבצעות פעולות שוטפות קבועות על האתר של הלקוח, משימות אלו עוברות בצורה מסודרת לצוות הבקרה של ממשל זמין, על מנת לזרז את הטיפול בנושא. כל פעולה שהלקוח מבקש לבצע בצורה קבועה על השרת, באמצעות צוות הבקרה, עוברת אישור של מנהל תחום האירוח ומקבלת אישור קבוע לביצוע הפעולה. פעולות חריגות מקבלות אישור ממנהל האירוח, כאשר כל בקשה נבחנת לגופה ועוברת לביצוע באמצעות

הבקרה או לחלופין באמצעות תחום האירוח. תחום האירוח אחראי על ביצוע גיבויים לשרתים ועדכוני מערכת הפעלה ואנטי וירוס.

5.15. **שימוש ב תעודת – SSL**

5.15.1. תשתיות ממשל זמין תומכות באתרים המוגנים באמצעות תעודת SSL. גורמי אבטחת המידע של ממשל זמין יכולים לדרוש את השימוש בתעודת SSL על ידי אתר הלקוח. ניתן להנפיק תעודות SSL דרך ממשל זמין. במקרה זה ממשל זמין ינפיק את תעודות ה –SSL עבור הלקוח - על ידי CA חיצוני – וזאת בהתאם לתנאי המכרז. באפשרות הלקוח לרכוש תעודות SSL על ידי גורם חיצוני. על התעודות להיות חתומות על ידי CA מוכר.

5.15.2. בכל מערכת בה יעבור מידע פרטי יש ליישם זאת על גבי תווך מוצפן.

5.15.3. קבלת פרטים מהמשתמש - דפים בהם מתבקש המשתמש למלא פרטים יכילו רכיב Captcha ויהיו מוגנים ב-SSL. לדוגמא דף "צור קשר".

5.16. **ארכיטקטורת אירוח**

5.16.1. מיקום רכיבי הפתרון - כל רכיבי הפתרון יתארחו ב-ISP.

5.16.2. שימוש בפתרונות מבוססי ענן פומבי יאושרו מראש על ידי תחום האירוח ומערך הגנה בסייבר של ממשל זמין עוד בשלב התנעת הפרויקט, כמו כן על המערכת לעמוד בהנחיות רשות התקשוב ("אבטחת מידע למעבר לענן ציבורי").

5.16.3. **תצורת מימוש** - הפתרון ימומש בתצורת Front/Back עם הפרדה מלאה לשלוש שכבות (Tier 3) תצוגה, BL, מסד נתונים. אם נדרש רכיב ניהול הוא יבנה בנפרד בצד האחורי של המערכת.

5.16.4. גישה שרת (server side) לרשת האינטרנט - לא תתאפשר גישה לשירותים ברשת אינטרנט מצד השרת.

5.16.5. **תמיכה בכרטיס חכם** - הפתרון יתמוך בהזדהות עם כרטיס חכם ו/או SSO על פי הנחיות ממשל זמין. הזדהות בכרטיס חכם הינה תנאי הכרחי לצורך גישה לממשק עדכון התוכן.

5.16.6. ממשקי ניהול תוכן וממשקי ניהול המערכת מחויבים להתארח בשרת נפרד ומוגנים על ידי כרטיס חכם.

5.16.7. **שימוש בשרותי רשת** - הטמעת web service בתוך הפתרון תעשה על פי תקן ws.gov.il

5.16.8. ניתן לעבות את המערך של השרת הקדמי באמצעות שימוש ב – NLB.

5.16.9. כל השרתים בתחום האירוח מוגדרים מאחורי NLB על מנת לייצר גמישות בהרחבת השירות הניתן ללקוחות.

5.16.10. במקרים בהם נדרשים צרכים חריגים מהארכיטקטורה הסטנדרטית של ממשל זמין, הגורמים המקצועיים בממשל זמין יתנו את הפתרון לאותו נושא.

5.16.11. כחלק ממדיניות אבטחת המידע והתפעול של ממשל זמין הוגדר ששום שרת לא יתפקד בשני תפקידים במערכת - לדוגמה שרת WEB עם שרת DB.

5.17. **מדיניות סיסמאות** – ע"פ המפורט במדיניות פיתוח מערכת מאובטחת.

5.18. **תוכן באתרים** – תוכן האתרים המתארחים בממשל זמין יהיה בסיווג בלמ"ס בלבד ובהתאם להגדרות רמו"ט (הרשות למדע וטכנולוגיה).

5.19. שמות המתחם צריכים להיות רלוונטיים לתוכן האתר וייקבעו בכפוף לאישור מנהל מערך ה-IT.

5.20. **הקשחות שרתים**

5.20.1. הקשחות השרתים בתחום האירוח מבוצע באמצעות נהלים מוגדרים לכל מערכת הפעלה ולכל מוצר הנתמך על ידי ממשל זמין.

5.20.2. כל חריגה מהנחיות ההקשחה של ממשל זמין – לצורך איפשור פונקציונאליות מסוימת והסרת הקשחה – מחייב קבלת אישור של גורמי אבטחת המידע והגנה בסייבר של ממשל זמין.

5.21. **תכנון ארכיטקטורת**

5.21.1. **מטרת/ מהות הפרויקט** – ארכיטקטורת האתר תותאם למטרת ומהות הפעילות בה אמור האתר לתמוך.

5.21.2. **קהל היעד** – בניית אתר תתבצע במטרה להתאימו לקהל היעד – הן מבחינת שפות, נגישות, מתן הסבר ועזרה וכיו"ב.

5.21.3. **הזדהות** – במידת הצורך ממשל זמין ידרוש הזדהות לצורך גישה לאתר.

5.22. **כימות (Sizing)** – בניית האתר – משלב האפיון ועד שלב ההשקה – תתבצע תוך התאמת משאבי האתר לאופי ועומס הפעילות בה אמור האתר לעמוד. טרם השקת האתר לאתר תתבצע בדיקת עומסים לווידוא התאמת משאבי האתר לעומסי הפעילות.

5.23. **תהליך עלייה לאויר** – תהליך זה מוסדר בנוהל אירוח אתרים בממשל זמין – לו נכתב נספח עבור לקוחות ממשל זמין. מסמך זה מתאר ומפרט את תהליך העליה לאויר, את שלביו ואת חלוקת האחריות בין ממשל זמין לבין הלקוח בכל שלב ושלב.

5.24. **תהליך העברת גירסה** – כל העברת גירסה תתבצע תוך שמירה על הוראות אבטחת המידע אשר נועדו להבטיח כי לא היה כל שינוי בקבצי הגירסה במהלך העברתה לממשל זמין בכלל ולא נכללו בקבצי הגרסה נוזקות אשר עלולות לחדור לתשתית האירוח ולסכן את פעילות ממשל זמין.

5.25. **מדיניות תקלות (עבודה מול בקרה / SLA)** – מדיניות הטיפול בתקלות בתשתית האירוח תיושם על עפי אמנת השירות המעודכנת של ממשל זמין

5.26. **מדיניות עבודה בממשל זמין**

5.26.1. **חדר מעדכנים** - ממשל זמין הקצה עמדות מעדכנים העומדות לרשות נציגי הלקוחות לצורך עדכון האתרים הנעשה ממתחמי ממשל זמין. על הלקוח יהיה לתאם את פעילות עדכון האתר וזאת בין היתר על מנת להקצות את עמדת

המעדכנים עבור הלקוח. פעילות העדכון תתבצע בשעות העבודה הרגילות (ימים א'-ה', בשעות 08:00-17:00, למעט ימי חגים ושבתון).

5.26.2. **אבטחה פיסית** – כתנאי לכניסת מעדכנים למתחמי ממשל זמין, יהיה עליהם לעבור בדיקה להתאמה בטחונית ולחתום על הצהרת התחייבות לשמירת סודיות והוראות אבטחת המידע.

5.27. **לוגים והתראות**

5.27.1. הפתרון יספק לוגים מפורטים והתראות על פעילות משתמשים ותהליכים בנוסף ללוגים המגיעים כברירת מחדל עם מערכת ההפעלה או המוצר התשתיתי.

5.28. **בקשות ובירורים טכניים**

5.28.1. לקוח המבקש לברר מידע טכני או יכולת טכנית על המערכת שלו, המתארחת בתחום האירוח, יוכל לפנות לצורך כך אל מנהל פרויקט התשתיות בממשל זמין.

5.29. **עדכון תוכן**

5.29.1. עדכון תוכן האתר מבוצע על ידי הלקוח בלבד. תחום האירוח אינו מתערב בניהול התוכן של אתר הלקוח וככלל לא מבצע בקשות של שינוי תוכן. במקרה בו קיימת בקשה חריגה, על הלקוח ליצור קשר עם מנהל הלקוח, על מנת שזה יאשר לתחום האירוח לבצע את השינוי. עדכון האתר מתבצע בשיטות שצוינו לעיל.

5.29.2. במסגרת מדיניות אבטחת המידע קיים Application FW שנדרש לעדכנו כאשר מוסיפים דפים חדשים לאתר. הבקשה לפתיחה של הדף מתבצע מול צוות הבקרה באמצעות שליחת פנייה לכתובת הדוא"ל: noc@ gov.il

5.30. **העלאת גרסאות**

5.30.1. העלאת גרסאות והחלפת רכיבי תשתית באתר הלקוח מתבצעת בתאום מראש מול מנהל הלקוח מטעם ממשל זמין, מנהל הלקוח יתאם את החלפת הגרסה מול הצוותים בממשל זמין. העלאת הגרסה מתבצעת אך ורק על ידי תחום האירוח. השקות אתרים ("עלייה לאויר") והעלאות גרסה לא יתבצעו בימי חמישי וביום הקודם לערבי חג ומועד.

5.31. **עדכוני אבטחה**

5.31.1. על השרת המתארח להיות מותקן בעדכוני התוכנה הקריטיים והעדכניים ביותר.

5.31.2. ממשל זמין מבצע מעת לעת עדכון מלא לכל מערכות ההפעלה והמוצרים המותקנים על השרתים.

5.31.3. ישנם מקרים חריגים, בהתאם לחומרת העדכון והסיכון שלו, אשר ממשל זמין יחליט להתקין את העדכון באופן מידי.

5.31.4. כל העדכונים מותקנים בשעות הלילה והשרתים מבצעים אתחול לאחר מכן. לא נשלחת הודעה ללקוח על ביצוע העדכונים על המערכות.

5.32. **עבודות תחזוקה**

5.32.1. עבודות תחזוקה בתשתית האירוח על השרתים הווירטואליים, על השרתים הפיסיים ועל המערכות התומכות, מבוצעת כל תקופת זמן המוגדרת מראש.

5.32.2. ממשל זמין מעדכן את הלקוחות על ביצוע עבודות אלה לפחות שבוע אחד מראש לפני תחילת העבודה .

6. אבטחת מידע

6.1. פיתוח ואירוח אתרים בממשל זמין יתבצע על פי קווי מדיניות אבטחת המידע ומדיניות פיתוח מערכת מאובטחת המתעדכנות מעת לעת ומפורסמות לעובדי ממשל זמין ולקוחותיו.

6.2. הוראות, הנחיות וכללי אבטחת המידע תשמרנה לאורך כל מחזור חיי האתר המתארח בממשל זמין. עוד בשלב ייזום אירוח אתר בממשל זמין יהיה על הלקוח לפרט את דרישותיו בהתאם למסמך הנחיות לכתיבת מסמך דרישות, תוך פירוט כל הדרישות הרגולטוריות, הדרישות הפונקציונאליות ודרישות אבטחת המידע ולספק למערך הגנה בסייבר את המידע הנדרש אודות הפרויקט.

6.3. **פיתוח האתר** – גם אם יתבצע על ידי חברה חיצונית - ייעשה תוך שמירה על כל הנחיות, הוראות וכללי אבטחת המידע אשר צריכים להיות מפורטים בנספח אבטחת מידע להתקשרות עם הספק החיצוני.

6.4. מערך סייבר ואבטחת המידע של ממשל זמין יהיה מעורב בכל שלבי מחזור החיים של פיתוח האתר - החל משלבי הייזום ודרך אפיון והתקנה, עד לחשיפת האפליקציה לגישה פומבית של המשתמשים בעולם.

6.5. בדיקת גרסאות האתר תתבצע על פי "*תכנית המסלולים*" לקיצור זמני העלייה לאוויר ותוך שמירה על הכללים לביצוע בדיקות חוסן.

6.6. היה ובדיקות החדירות ובדיקות החוסן יתבצעו על ידי צוות בדיקות אפליקציה במערך הגנה בסייבר בממשל זמין, משך הבדיקות ומועדן ייקבע על פי מאפייני האתר ומרכיביו ועל פי מוכנות האתר לשלב הבדיקות.

6.7. **סקר קוד ובדיקות חוסן** - כל רכיבי המערכת יעברו בדיקות חדירות/חוסן וסקר קוד על ידי חברה ישראלית שאושרה מראש על ידי ממשל זמין. הבדיקות בפועל יתבצעו מאתר ממשל זמין. דו"ח ממצאים יועבר לאישור ממשל זמין.

6.8. **טיפול בממצאי סקר קוד/בדיקת חוסן** – יש לטפל בכל הממצאים לפני קבלת אישור עליה לאוויר.

6.9. טרם עליית האתר לאוויר והשקתו, יהיה על מערכות אבטחת המידע 'ללמוד' את האתר. משימה זו תתבצע על ידי הלקוח ובאחריותו - ובהנחיית תחום אירוח ותחום יישומי אבטחת מידע.

6.10. הנחיות אבטחת המידע בתחום הצפנת המידע:

6.10.1. על מנת לשמור על רמת אבטחה גבוהה בממשל זמין, יש צורך לעשות שימוש בשיטות הצפנה (Cipher Suite) וגרסאות SSL מעודכנות.

6.10.2. פרטים נוספים לגבי גירסת SSL, חוזק ושיטת הצפנה והגדרות נוספות ניתן לקבל מתחום אירוח בשלב בדיקת ההיתכנות.

6.11. בפיתוח אתר המנגיש מאגרי מידע קיימת חובת קיום מנגנון למניעת ריבוי בקשות במטרה למנוע "*שאיבת מידע*".

6.12. יש ליישם הנחיות אלו על כלל השרתים, רכיבי הסינון ורכיבי הרשת בכל הרשתות והתשתיות בממשל זמין.

6.13. **הלבנת קבצים** – כל קבצי האתר וגרסאותיו – הן בשלב ההקמה והן בשלבי העדכון ואחרים – יעברו תהליך 'הלבנה' וזאת כתנאי לטעינתם לתשתיות ממשל זמין.

6.14. **התקשרות עם ספקי חוץ:**

6.14.1. כל התקשרות עם ספקי חוץ תתבצע על פי הוראות נהלי ממשל זמין המגדירים את אופן הקמת הממשק מול ספקים חיצוניים – החל מבדיקות הישימות של ציוד חדש (נוהל PoC), רכישת והתקנת תוכנות ומוצרים ונוהל תחזוקת ציוד לאחר שהותקן במתחמי ממשל זמין.

6.14.2. בהתקשרות עם ספק חיצוני יש להדגיש את אחריותו של הספק החיצוני לעמוד בדרישות אבטחת המידע של ממשל זמין ובכללן:

- שמירת עקרונות אבטחת המידע הנדרשים הן ממוצרים ותוכנות אשר יותקנו בתשתיות ממשל זמין והן במהלך רכש פתרונות פיתוח אשר יתארחו בתשתיות הארגון.
- מניעת קיום פגיעויות אבטחתיות – ובכללן "דלתות אחוריות" - ברכיב המפותח או מותקן על ידי הספק.
- דיווח לממשל זמין אודות פגיעויות אשר נתגלו ברכיבים המפותחים על ידי הספק.
- דיווח על אירועי סייבר ואבטחת מידע במתחמיו.
- חתימה על הצהרת התחייבות לשמירה על סודיות והוראות אבטחת המידע וזאת בין היתר גם כתנאי לכניסה למתחמי ממשל זמין.

6.15. בעת הטמעת פתרון בענן, על המערכת לעמוד בהנחיות רשות התקשו"ב.