Supplier Control Obligation (SCO)

אבטחת מידע וסייבר (ICS)

אזור/תפקיד מפוקח	תיאור הפיקוח	מדוע זה חשוב
1. שימוש מאושר	על הספק לוודא שהמידע ונכסים קשורים אחרים מוגנים, מנוצלים ומטופלים כהלכה. כללים לשימוש מקובל ונהלים לטיפול במידע ובנכסים קשורים אחרים יזוהו, יתועדו וייושמו. על עובדי ספקים, לרבות קבלנים, קבלני משנה, מעבדי משנה במסגרת תחומי האחריות שלהם שעושים שימוש או מקבלים גישה למידע של הארגון ונכסים קשורים אחרים להיות מודעים לדרישות אבטחת המידע לצורכי הגנה על המידע ולדרישות הטיפול במידע של הארגון ובנכסים קשורים אחרים. עליהם ליטול אחריות על השימוש שהם עושים במתקני עיבוד מידע כלשהם. על הארגון לקבוע מדיניות ספציפית העוסקת בשימוש מקובל במידע ובנכסים קשורים אחרים ולשתף אותה עם כל מי שעושה שימוש במידע או מטפל בו ובנכסים קשורים אחרים. על הספק לנקוט באמצעים הולמים כדי להבטיח ציות לדרישות השימוש המקובל. יש לשקול את הנושאים הבאים: • שימוש באינטרנט. • שימוש בפתרון תוכנה כשירות (SaaS). • שימוש במאגרי קוד ציבורי. • שימוש בתוספים מבוססי דפדפן ובתוכנות חינמיות/שיתופיות. • שימוש ברשתות חברתיות. • שימוש בכתובת דואר אלקטרוני ארגונית. • שימוש בהודעות מידיות. • שימוש בציוד IT שמסופק על ידי הספק. • שימוש בציוד IT שאינו מסופק על-ידי הספק (כגון, יישום מסגרת של 'הבא מכשיר משלך'). • שימוש בהתקני אחסון ניידים/נשלפים. • תחומי אחריות בעת טיפול, שמירה ואחסון נכסי מידע של Barclays. • פלט של ערוצי זליגת נתונים; וכן • סיכונים ותוצאות הנובעים משימוש לרעה בפריטים הנ"ל ו/או כל תוצאה בלתי חוקית, מזיקה או פוגענית הנובעת משימוש לרעה כגון זה.	דרישת לשימוש מקובל עוזרת לבסס את סביבת הפיקוח שמגנה על נכסי המידע.
2. אבטחת גבולות ורשת	על הספק לוודא שכל המערכות והאפליקציות המופעלים על ידו ו/או על ידי קבלני/מעבדי משנה ומספקים תמיכה לשירותי Barclays מוגנים מפני איומי רשת – נכנסים ויוצאים. יש ליישם אמצעי פיקוח כדי לוודא שאבטחת מידע ברשתות והגנה על שירותים מחוברים מפני גישה בלתי מורשית פעילות. על הספק לזהות, להגן ולהגיב לכל התרעה ופריצת אבטחה.	אי יישום עיקרון זה עלול לגרום לחשוף רשתות פנים או חוץ ארגוניות למתקפות שמשימתן היא קבלת גישה לשירות או לנתונים המאוחסנים בו.

	על אמצעי אבטחת רשת מבטיחים הגנה על מידע ברשתות ובמתקני עיבוד המידע התומכים בהן לכלול, ללא הגבלה, את התחומים הבאים: • הקפדה על רישום מלאי עדכני של כל גבולות הרשת הארגונית (באמצעות ארכיטקטורת רשת/דיאגרמה) וביצוע סקירה פעם בשנה לפחות. • תיעוד, אימות ואישור חיבורים חיצוניים לרשת הספק לפני הקמת החיבורים, למניעת פרצות אבטחה. • הגנה על רשתות הספק באמצעות יישום עקרונות הגנה יסודית (כגון פילוח הרשת, הפעלת פתרונות חומת אש וכו'). • על הספק לפרוס פתרונות טכנולוגיית למניעת חדירות לרשת כדי שיוכל לזהות ולמנוע תעבורה נכנסת/יוצאת זדונית ולוודא שמסדי נתונים חתומים פועלים באופן מיטבי ובהתאם לשיטות העבודה הטובות ביותר בתעשייה, תוך החלת עדכונים המתקבלים מספק הפתרונות במועד. • על הספק לוודא שקישוריות פרטית בין שירותי ענן וירטואליים פרטיים (VPC) לרשתות מקומיות של צד שלישי תהיה מוצפנת, לצד מניעת חשיפה לרשת האינטרנט הציבורית. • על תעבורת רשת האינטרנט לעבור דרך שרת Proxy שתצורתו מסננת חיבורים לא מורשים. • יש לקיים הפרדה לוגית בין יציאות/ממשקי ניהול התקנים לבין רשת LAN/ תעבורת משתמשים ויישום אמצעי פיקוח הולמים. • יש לקיים תקשורת מאובטחת בין התקנים ותחנות/מסופי ניהול. • יש לוודא כי תהליכי הרישום והניטור כוללים זיהוי והתראות בשל פעילויות חשודות (באמצעות זיהוי דפוסי התנהגות וסימנים המעידים על גורמים מפעילים בסיכון), כגון באמצעות פתרון SIEM. • יש להצפין את החיבור בין הרשת הארגונית לשירותי הענן/מרכזי הנתונים באמצעות יישום פרוטוקול מאובטח. יש להצפין את נכסי המידע/הנתונים במעבר ברשת הארגונית של הספק מסוג WAN (Wide Area Network). • על הספק לעיין בכללי חומת האש (חומת אש חיצונית ופנימית) ולבחון אותם פעם בשנה לפחות. • על הספק לוודא שהגישה לרשת הפנים ארגונית מנוטרת באמצעות יישום אמצעי פיקוח המאפשרים גישה הולמת לרשת. • כל גישה אלחוטית רשת כפופה לאישור, אימות, פילוח ודרך פרוטוקולי הצפנה רבי עוצמה כדי למנוע פרצות אבטחה. • על הספק לפרוס רשת נפרדת (באופן לוגי) עבור השירותים המסופקים ל-Barclays. על הספק לוודא שכל השרתים והאפליקציות המשמשים לאספקת שירותים ל-Barclays אינם נפרסים ברשתות לא מהימנות (רשתות מחוץ להיקף האבטחה של ארגון הספק, שאינן בשליטתו הניהולית, כגון רשתות עם חיבור לאינטרנט). על ספק שמארח מידע של Barclays (לרבות קבלני/מעבדי משנה) במרכז נתונים או בענן להחזיק בהסמכת Best Industry Practice לניהול אבטחת רשת.	

	רשת T2 ו-T3 – • יש להקפיד על הפרדת רשת T2 מבחינה לוגית מהרשת הארגונית של הספק באמצעות חומת אש, כדי לוודא שכל התעבורה הנכנסת והיוצאת תוגבל ותנוטר. • על תצורת הניתוב להבטיח חיבורים לרשת של Barclays בלבד ואין לנתב אותה לרשתות אחרות של הספק. • יש להגדיר את נתב הקצה/Edge ('הק"מ האחרון של החיבור) המתחבר לשער Extranet של Barclays, תוך יישום תפיסה של הגבלת הפיקוח ביציאות, בפרוטוקולים ובשירותים. ○ יש לוודא כי תהליכי הרישום והניטור כוללים זיהוי והתראות בשל פעילויות חשודות (באמצעות זיהוי דפוסי התנהגות וסימנים המעידים על גורמים מפעילים בסיכון), כגון באמצעות פתרון SIEM. **על ספק שהוא צד שלישי להבטיח שכל המערכות והאפליקציות המשמשות לאספקת השירותים הנחשבים לדעתה של Barclays כבעלי סיכון גבוה, מופרדים ברשת. יש להבטיח הפרדה למחיצות של אפליקציות עסקיות ורכיבי הליבה של התשתית (למעט תשתיות קריטיות משותפות ומתפשטות) אל תוך מקטע הרשת, תוך שימוש בטכנולוגיות אבטחה שאושרו על ידי Barclays (חומות אש או טכנולוגיות שוות ערך אחרות) כדי לעמוד בעקרונות שלהלן.** i. יש לנקוט בגישה של הפרדה למקטעים כדי להגביל את החשיפה לסיכון, לעכב תנועה ברשת ולצמצם את הסיכון לשידור רשת. יש לפרוס אפליקציות למקטעים עצמאיים כדי להגביל את רמת הסיכון ככל האפשר. דוגמה: אזור לביצוע תשלומים באופן מהיר יותר. יש להקפיד על פריסה של כל התשתיות והנתונים הקשורים לאפליקציות עסקיות באזור יישומים מאובטח ועצמאי (כשבדבר אפשרי), עם הפרדה מהרשת הפנימית של Barclays, תוך שימוש בטכנולוגיית אכיפת CSO מאושרת (כגון חומות אש של הרשת, פתרון הפרדה מאושר). הערה – תרחישים מסוימים עשויים להצדיק פיצול בין רכיבים, כגון בין האפליקציה למסד הנתונים ולפרוס אותם באזורים שונים, למשל, בעת מינוף של פלטפורמות משותפות. יש לבצע הערכה של כל אפליקציה בנפרד, כשהגישה המתאימה ביותר מוגדרת ומאושרת על ידי יועץ אבטחה של CSO. ii. יש להקפיד על הפרדה פיזית או לוגית של השירותים. ניתן לשתף את מארג הרשת הבסיסי (כגון כבלים/מתגים) עם אפליקציות ושירותים אחרים, כלומר, ניתן להגדיר מקטעים באופן לוגי, ללא צורך באכיפת הדרישה לביצוע הפרדה פיזית משאר רכיבי הרשת של Barclays. iii. על אזורי האפליקציות להגביל זרימות תעבורה אל ומאזורים אחרים (כולל רשת CIPE פנימית), על בסיס אלה הדרושים לתפעול השירות וכלי ניהול, ניטור ואבטחה מאושרים. על התצורות לקבוע יציאות, פרוטוקולים וכתובות IP ספציפיים עבור נתיבי תקשורת מורשים – יש להגביל את כל שאר רכיבי התקשורת כברירת מחדל. יש להימנע מכללים המכילים טווחים ולאשר אותם כחריגים, רק לצורכי הבטחה שרק דרישות הקישוריות המינימליות יהיו זמינות. iv. יש להפריד את הגורמים המכילים באופן יציב, תוך יישום אמצעי פיקוח לוגיים רבי עוצמה המונעים תנועה אופקית בין הגורמים המכילים על מנת לאכוף בידוד. אין לאפשר מצב שבו פגיעה בגורם מכיל אחד תוביל לפגיעה בגורמים מכילים אחרים הפועלים באותו מארח/אשכול. v. על כל יישום של הפרדה להציע יכולת מפתח לניהול כללי מדיניות מרכזיים הכוללים פונקציונליות (או אינטגרציה) כדי לבצע אימות ולדווח על ציות לכללי המדיניות (יש לעיין במסמך שכותרתו 'תאימות חומת אש') ולהבטיח תיעוד של שינויים כלשהם ביומן הביקורת.	

	vi. יש להפעיל פיקוח/בקרה במצב שבו הדבר אפשרי/מעשי. vii. יש ליישם הפרדה באופן בטוח מפני כשלים, כגון, במקרה של כשל היכולת, יישומו כללים מאושרים לחסימה/לאישור תעבורה. viii. כל תעבורה בין מערכות הייצור למערכות שאינן מערכות ייצור באזורי האפליקציות מחייבת היתר ויש לתעד אותה. **הנחיות ללקוח של שירותי ענן (ספק) שמשמשות לצורכי אספקת שירותים ל-Barclays.** לקוח שירותי הענן (CSC) נדרש לוודא פריסה של אמצעי הפיקוח נאותים לצורכי אבטחת רשת כדי להבטיח את רמת האבטחה של השירותים המסופקים ל-Barclays – • על לקוח שירותי הענן (CSC) להגדיר את הדרישות להפרדת רשתות כדי להבטיח בידוד דיירים בסביבה המשותפת של שירותי הענן ולוודא שספק שירותי הענן מציית לדרישות אלה. • על מדיניות בקרת הגישה של לקוח שירותי הענן בעת שימוש בשירותי רשת צריכה לציין מהן הדרישות לגישת משתמשים עבור אחד משירותי הענן. *לתשומת לבך: המונח 'רשת', המשמש במסגרת אמצעי פיקוח זה, מתייחס לכל רשת שאינה רשת של Barclays, באחריות הספק, לרבות רשת בבעלות קבלן המשנה של הספק.*	
3. זיהוי מניעת שירות	על הספק לשמר את יכולתו לזהות ולהתגונן מפני מתקפות מניעת שירות (DoS) ומתקפות מניעת שירות מבוזר (DDoS). על הספק לוודא שערוצים המחוברים לאינטרנט או ערוצים פנים ארגוניים המספקים תמיכה לשירותים המסופקים ל-Barclays זוכים לאבטחה הולמת מפני מתקפות DDoS/DoS כדי להבטיח זמינות. אם הספק מארח **מערכות ואפליקציות המספקים שירותים** ומחזיק ברשותו נתונים של Barclays או מסווג קטגוריות העמידות 0 או 1, עליו ליישם אמצעי אבטחה הולמים כדי להתגונן מפני מתקפות DoS ולהבטיח זמינות.	אי יישום של עקרות זה עלול לחשוף את Barclays ואת ספקיה בפני מתקפות מניעת שירות ולמנוע את האפשרות להתמודד בהצלחה עם המתקפות.
4. עבודה מרחוק (גישה מרחוק)	על הספק להבטיח רמה הולמת של אבטחת מידע בעת יישום מסגרת של עבודה מרחוק. יש ליישם אמצעי אבטחה שנועדו להגן על מידע שהגישה אליו ועיבודו מבוצעים חוץ למרחבים הפיזיים של הארגון, במסגרת עבודה מרחוק. על הספק להבטיח מתן הוראות מתאימות לכל עובדיו לגבי עבודה מהבית. **גישה מרחוק לרשת של Barclays** גישה מרחוק לרשת של Barclays באמצעות שימוש באפליקציה Barclays Citrix אינה מוקצית כברירת מחדל. כדי לגשת לרשת של Barclays ממיקומים לא מאושרים/מחוץ למשרד/מהבית, ובכל מקרה של קבלת גישה מרחוק, נדרש אישור מראש והרשאה של Barclays (צוות TPSecM במשרד סמנכ"ל האבטחה – (externalcyberassurance@barclayscorp.com)). על הספק לוודא יישום ופריסה של אמצעי הפיקוח הבאים כדי לאפשר גישה מרחוק: • הגישה לרשת של Barclays מחייבת שימוש באסימון RSA (רך) והפעלת גרסה נתמכת של האפליקציה Citrix Workspace; Barclays תספק את הפרטים המתאימים	אמצעי פיקוח על גישה מרחוק עוזרים לוודא שלא מתבצע חיבור מרחוק של מכשירים בלתי מורשים או לא בטוחים לסביבת המחשוב של Barclays.

	• על הספק להקפיד להחזיק תיעוד עדכני ומדויק לגבי עובדים שלהם הצדקה עסקית ואישור לעבוד מרחוק/באופן היברידי, לרבות קבלני/מעבדי משנה. • **על הספק לבצע התאמה רבעונית של כל העובדים שמקבלים גישה מרחוק ולאחר מכן להעביר את התוצאות ל-Barclays (לצוות TPSecM במשרד סמנכ"ל האבטחה – externalcyberassurance@barclayscorp.com)).** • Barclays תשבית אישורי אימות לאחר מתן הודעה כי הגישה אינה נחוצה עוד (כגון לאחר פיטורי עובד, הקצאה מחדש של פרויקט וכו') **לא יאוחר מעשרים וארבע (24) שעות מתאריך היציאה/יום העבודה האחרון במשרד (LDIO)** • Barclays תשבית באופן מיידי אישורי אימות לאחר אי שימוש לפרק זמן מסוים באישורים כגון אלה (תקופת אי השימוש לא תעלה על חודש אחד). • על הספק לוודא שתצורת נקודת הקצה המשמשת לביצוע חיבור מרחוק למערכות מידע של Barclays מאובטחת (כגון, רמת טלאי תיקון, מצב הפתרון למניעת תוכנות זדוניות וכו'). • על שירותים עם גישה להדפסה מרחוק באמצעות אפליקציית Barclays Citrix לקבל אישור של Barclays (צוות TPSecM במשרד סמנכ"ל האבטחה – **externalcyberassurance@barclayscorp.com**). על ספק להחזיק רשומות ולבצע התאמה על בסיס רבעוני. • **אין לאפשר גישה לסביבה של Barclays ו/או לנתונים של Barclays המאוחסנים בסביבה המנוהלת על-ידי הספק באמצעות מכשירים אישיים/BYOD (הדרישה מוגבלת למחשבים ניידים/מחשבים שולחניים וחלה על עובדי הספק, יועצים, עובדים זמניים, קבלנים ושותפי שירות מנוהלים, קבלני/מעבדי משנה).** הערה: גישה מרחוק לרשת ולנתונים של Barclays אסורה, אלא אם קיבלה אישור מפורש מ-Barclays. **גישה מרחוק לסביבה/לרשת של הספק** גישה מרחוק לסביבה המנוהלת על-ידי הספק לצורך אספקת שירות, הכוללת נתונים של Barclays המאוחסנים ו/או מעובדים בסביבה או ברשת של הספק. על הספק לוודא שאמצעי הפיקוח הבאים מיושמים ונפרסו לרשת הארגונית של הספק לצורך מתן אפשרות לגישה מרחוק. • יש לוודא הצפנה מתקדמת של פעולות כניסה מרחוק לרשת הספק בעת העברת נתונים ולייישם שימוש באימות רב-גורמי. • הספק עשוי להשתמש בשולחן עבודה וירטואלי לצורכי גישה מרחוק • על הספק להחזיק ברשומות עדכניות של משתמשים שעובדים מרחוק או באופן היברידי. • **על הספק לבצע התאמה של כל המשתמשים מרחוק בהתאם לצירי הזמן של הספק** • הספק יבטל אישורי אימות לאחר מתן הודעה כי הגישה אינה נחוצה עוד (כגון לאחר פיטורי עובד, הקצאה מחדש של פרויקט וכו') **לא יאוחר מעשרים וארבע (24) שעות מתאריך היציאה/יום העבודה האחרון במשרד (LDIO)**	

<table>
<tr><td></td><td>

- **אין לאפשר גישה לנתונים של Barclays המאוחסנים בסביבה המנוהלת על-ידי הספק באמצעות מכשירים אישיים/BYOD (הדרישה מוגבלת למחשבים ניידים/מחשבים שולחניים וחלה על עובדי הספק, יועצים, עובדים זמניים, קבלנים ושותפי שירות מנוהלים,קבלני/מעבדי משנה).**

על הספק למסור לעובדיו את הכללים העוסקים בעבודה מהבית, לרבות כללי 'עשה ואל תעשה'.

אין ליישם מסגרות עבודה מרחוק (כולל עבודה מהבית) במהלך פעילות עסקית רגילה, כשצדדים שלישיים נדרשים על פי חוזה לספק שירותים ממיקום ייעודי של הבנק או ממיקום ייעודי של ספק או כשחלות דרישות רגולטוריות. עם זאת, הוראה כגון זו מותרת במסגרת תוכניות המשכיות עסקית של צדדים שלישיים במקרה של התאוששות מאסון/משבר/תגובה מגפה בהסכמה של Barclays ובהתאם לכל דרישות האבטחה המחייבות המהוות חלק בלתי נפרד מההסכם החוזי, בהקשר של עבודה מרחוק.

</td><td></td></tr>
<tr><td>5. ניהול יומן אבטחה</td><td>

על הספק ליישם מסגרת מבוססת היטב של ביקורות וניהול יומנים. על המסגרת לכסות מערכות IT מרכזיות, כולל אפליקציות, ציוד עבודה ברשת, התקני אבטחה ושרתים שבהם נרשמים אירועי מפתח. כדי לתעד אירועים, להפיק ראיות, להבטיח את שלמות המידע ביומן, יש להקפיד שיומני הרישום אינם ניתנים לשינוי, למנוע גישה בלתי מורשית, לזהות אירועי אבטחת מידע שעלולים להוביל לתקריות אבטחת מידע ולספק תמיכה מלאה בחקירות. על הספק לוודא כי יומני הרישום מרוכזים ומאובטחים כהלכה מפני פעולות של חבלה ו/או מחיקה, ונשמרים על ידו למשך פרק זמן מינימלי של 12 חודשים או לפרק הזמן שנקבע במסגרת הדרישה הרגולטורית החלק, הארוכה מבין שתיהן.

קטגוריה	מערכות/שירותים בעלי רמת השפעה נמוכה	מערכות/שירותים בעלי רמת השפעה בינונית	מערכות/שירותים בעלי רמת השפעה גבוהה
שמירת יומנים	3 חודשים	6 חודשים	12 חודשים

על מסגרת ניהול יומני אבטחה לכסות את התחומים הבאים:

- על הספק להגדיר את התפקידים ואת תחומי האחריות של יחידים וצוותים שייטלו חלק בניהול היומנים.
- איסוף, ניהול וניתוח יומני ביקורת של אירועים כדי לעזור במאמצי ניטור, זיהוי, הבנה ו/או התאוששות ממתקפה.
- קיום תהליכי רישום מערכת לצורכי הכללת מידע מפורט, כגון מקור אירוע, תאריך, משתמש, חותמת זמן, כתובות מקור, כתובות יעד ורכיבים שימושיים אחרים.
- יומני אירועים לדוגמה עשויים לכלול:
  - IDS/IPS, נתב, חומת אש, Web Proxy, Remote Access Software (VPN), שרתי אימות, אפליקציות, יומני מסד נתונים.

</td><td>אי יישום אמצעי פיקוח זה ימנע מהספק לזהות ולהגיב במקרה של שימוש בלתי הולם או זדוני בשירות או בנתונים תוך פרק זמן סביר.</td></tr>
</table>

	○ כניסות שבוצעו בהצלחה, ניסיונות כניסה כושלים (למשל, בשל מזהה משתמש או סיסמה שגויים), יצירה, שינוי ומחיקה של חשבונות משתמשים ○ יומני רישום של שינויי תצורה. • שירותי Barclays הקשורים לאפליקציות עסקיות ולמערכות תשתית טכניות שעליהן יש להפעיל את הרישום המתאים ואת שיטות העבודה המומלצות בתעשייה, לרבות אלה שמיושמים באמצעות מסגרות של מיקור חוץ או מופעלים 'בענן'. • סנכרון חותמות זמן בין יומני אירועים למקור נפוץ ומהימן • הגנה על יומני אירועים הקשורים לאבטחה (כגון, באמצעות הצפנה, MFA, בקרת גישה וגיבוי). • פריסה של כלי ניתוח מידע אבטחה וניהול אירועים (SIEM) או של יומן רישום, לצורך התאמות וניתוח של יומנים. • פריסה של כלים בהתאם לצורך לביצוע צבירה מרכזית בזמן אמת והתאמה של פעילויות חריגות, התראות רשת ומערכות, כמו גם מודיעין רלוונטי לגבי אירועים ואיומי סייבר ממקורות מרובים, כולל מקורות פנימיים וחיצוניים, כדי לזהות אותם טוב יותר ולמנוע מתקפות סייבר מרובות פנים. • על ניתוח היומן לכסות את הניתוח והפרשנות של אירועי אבטחת מידע כדי לעזור במאמצים לזהות פעילות חריגה או דפוסי התנהגות חריגים אשר יכולים להוות סמנים המצביעים על פגיעה. • על האירועים המרכזיים שנרשמו לכלול את אלה עם פוטנציאל להשפיע על הסודיות, השלמות והזמינות של השירותים המסופקים ל-Barclays, העשויים לעזור במאמצי הזיהוי או החקירה של אירועים ו/או הפרות של זכויות הגישה המתרחשות ביחס למערכות הספק. • יש לבדוק מעת לעת ולוודא שהמסגרת עומדת בכל הדרישות לעיל. **הנחיות ללקוח של שירותי ענן (ספק) שמשמשות לצורכי אספקת שירותים ל-Barclays.** לקוח שירותי הענן (CSC) נדרש לוודא פריסה של אמצעי אבטחה נאותים כדי להבטיח את רמת האבטחה של השירותים המסופקים ל-Barclays – • על לקוח שירותי הענן להגדיר ולתעד את דרישותיו לרישום אירועים ולוודא שספק שירותי הענן מציית לדרישות אלה. • אם מתבצעת הקצאה של פעולה עם הרשאה ללקוח שירותי ענן, יש לרשום את הפעולה ואת תוצאותיה. על לקוח שירות הענן לקבוע אם יכולות הרישום ביומן של ספק שירותי הענן נאותות או אם על לקוח שירותי הענן ליישם יכולות רישום יומן נוספות. • על לקוח שירותי הענן לבקש מידע אודות סנכרון השעון המשמש את המערכות של ספק שירותי הענן. • על לקוח שירותי הענן לבקש מידע מספק שירותי הענן לגבי יכולות ניטור השירות הזמינות עבור כל שירות ענן.	
6. הגנה מפני תוכנות זדוניות	בהתאם לנוהלי שיטות העבודה הטובות ביותר בתעשייה (Best Industry Practice), על הספק לקבוע מדיניות ונהלים שמיועדים לתמוך בתהליכים עסקיים ובאמצעים טכניים שיושמו, על מנת למנוע הפעלה של תוכנות זדוניות בכל סביבת ה-IT. על הספק לוודא שהגנה מפני תוכנות זדוניות מוחלת על כל נכסי ה-IT הישימים בכל עת, כדי למנוע הפרעה לשירות או פרצות אבטחה.	פתרונות למניעת שימוש בתוכנות זדוניות חיוניים להגנה על נכסי המידע של Barclays מפני קודים זדוניים.

	על הגנה מפני תוכנות זדוניות לכלול, ללא הגבלה, את התחומים הבאים: • ניהול מרכזי של אמצעים למניעת שימוש בתוכנות זדוניות על מנת לנטר ולהגן באופן רציף על סביבת ה-IT של הארגון. • יש לוודא שהתוכנה למניעת שימוש בתוכנות זדוניות מעדכנת את מנוע הסריקות שלה. • עדכון מסד נתונים של חתימות על בסיס קבוע • שליחת כל אירוע של זיהוי התוכנה זדונית לכלי הניהול של תוכנות זדוניות ואת שרתי יומני האירועים לצורכי ניתוח ומתן התראות. • על הספק ליישם אמצעי פיקוח מתאימים כדי להתגונן מפני תוכנות זדוניות ומתקפות במכשירים ניידים המשמשים לצורכי השירותים המסופקים ל-Barclays. • שער הדואר האלקטרוני סורק את כל הודעות הדואר הנכנסות, היוצאות והפנים ארגוניות, לרבות קבצים מצורפים וכתובות URL, כדי לאתר סימנים לתוכן זדוני או מזיק. לתשומת לבך: על אמצעים למניעת שימוש בתוכנות זדוניות לכלול (ללא הגבלה), קודים של מכדירים ניידים בלתי מורשים, וירוסים, תוכנות ריגול, תוכנות פריצת מפתחות, תוכניות Botnet, סוסים טרויאניים וכו'.	
8. אבטחת נקודות קצה	על הספק לאמץ גישה אחודה לניהול נקודות קצה כדי להבטיח שנקודות הקצה המשמשות לצורכי גישה לרשת של Barclays או לצורכי גישה ו/או עיבוד של נכסי מידע/נתונים של Barclays, עמידות ומאפשרות הגנה הולמת מפני מתקפות זדוניות. יש לפרוס את שיטות העבודה המומלצות בתעשייה ועל אמצעי האבטחה שמיושמים בנקודות הקצה לכלול (ללא הגבלה): • הצפנה מלאה של כונני דיסק קשיח. • השבתת כל התוכנות/השירותים/היציאות שאינם נחוצים. • השבתת זכויות גישה מנהליות עבור משתמשים מקומיים. • עובדי הספק לא יורשו לשנות הגדרות בסיסיות כגון ערכות טיפול המהוות ברירת מחדל, חלוקה למחיצות במערכת, שירותי ברירת מחדל, תוכנות אנטי-וירוס וכו'. • השבתת יציאות USB לצורכי העתקת מידע/נתונים של Barclays לכונני מדיה ניידים • הקפדה על עדכון תוכנות אנטי-וירוס לגרסאות העדכניות ביותר והתקנת כל טלאי האבטחה הדרושים. • השבתת האפשרות לבצע הדפסה ברקע • כלי למניעת נתונים, להגנה מפני הפרות שחלות על נתונים של Barclays • על הספק לחסום כל יכולת 'זליגה' של נתוני Barclays לאתרים של רשתות חברתיות, שירותי דואר אלקטרוני ואתרים שיכולים לאחסן מידע, כגון, אך אינן מוגבלים ל-Google, Dropbox, iCloud. • השבתת יכולות שיתוף/העברה של נתוני Barclays באמצעות שימוש בכלים/תוכנות להעברת הודעות מידיות. • זיהוי, עצירה ותיקון נוכחות ו/או שימוש בתוכנות בלתי מורשות, לרבות תוכנות זדוניות.	אי יישום של אמצעי פיקוח אלה עלולה לחשוף את הרשת ואת נקודות הקצה של הספק למתקפות סייבר.

	• נעילת אפשרות לפסקי זמן של מסכים, הגבלת חיבורי TCP IP לרשת הארגונית בלבד, יישום סוכני אבטחת EPS מתקדמים לצורכי זיהוי דפוסי התנהגות חשודים לתשומת לבך: יש להשבית את יכולת השימוש בכונני מדיה ניידים/בהתקני אחסון ניידים כברירת מחדל ולאפשר את השימוש בהם רק לצרכים עסקיים לגיטימיים. על הספק לשמור תמונות או תבניות מאובטחות עבור כל המערכות בארגון, בהתאם לתקני התצורה המאושרים של הארגון. יש להגדיר את התצורה של כל פריסת מערכת חדשה או קיימת שנפגעה באמצעות שימוש בתמונות או בתבניות מאושרות. כשהגישה דרך נקודות קצה (מחשבים ניידים/מחשבים שולחניים) מוענקת עבור הרשת של Barclays באמצעות שימוש באפליקציה Barclays Citrix באינטרנט, על הספק להתקין את הכלי End Point Analysis (EPA) המסופק על ידי Barclays כדי לאמת את רמת האבטחה של נקודת הקצה ואת רמת התאימות של מערכת ההפעלה – רק מכשירים שעוברים את בדיקות ניתוח נקודת הקצה יקבלו גישה מרחוק לרשת של Barclays באמצעות שימוש באפליקציה Barclays Citrix. אם הספק אינו יכול להתקין את הכלי EPA או להשתמש בו, יש לדווח על כך למנהל הקשר על Barclays/לצוות תמיכת ה-IT של Barclays/לצוות TPSecM. **מכשירים ניידים המשמשים לצורכי אספקת השירותים של Barclays –** • על הספק לוודא שהוא מיישם את היכולות לניהול נקודות קצה אחודות (UEM) או ניהול מכשירים ניידים (MDM) כדי לפקח ולנהל באופן מאובטח מכשירים ניידים לאורך כל מחזור החיים שלהם שבמהלכו הם מקבלים גישה ו/או מכילים מידע מסווג של Barclays, על מנת לצמצם את הסיכון לפגיעה בנתונים. • על הספק לוודא שברשותו יכולות לנעול ולמחוק מרחוק מכשירים ניידים ולהשתמש בהן כדי להגן על מידע במקרה של פריצה, אובדן או גנבה של מכשיר • יש להצפין נתונים של Barclays המאוחסנים ו/או מעובדים במכשירים ניידים • על הספק לוודא שהמכשירים הניידים אינם מושרשים ולהקפיד על יישום מדיניות אימות חזקה	
9. מניעת זליגת נתונים	על הספק ליישם מסגרת יעילה שאושרה על-ידי ההנהלה כדי לאבטח את נתוני Barclays זליגה/חילוץ ולכלול (ללא הגבלה) ערוצים לזליגת נתונים: - • העברה בלתי מורשית של מידע אל מחוץ לרשת הפנימית/לרשת הספק ○ כתובת דוא\"ל ○ אינטרנט/שער אינטרנט (כולל אחסון מקוון ודואר באינטרנט) ○ DNS • אובדן או גנבה של נכסי מידע של Barclays במדיה אלקטרונית ניידת (כולל מידע אלקטרוני המאוחסן במחשבים ניידים, במכשירים ניידים ובמדיה ניידת). • העברה לא מורשית של מידע לאמצעי מדיה נייד באמצעות חיבור (כגון טורי, USB) ואלחוטי (כגון Wi-Fi ,Bluetooth). • החלפת מידע באופן לא מאובטח עם צדדים שלישיים (קבלני/מעבדי משנה). • הדפסה או העתקה של מידע באופן בלתי הולם.	יש להפעיל באופן יעיל את אמצעי הפיקוח המתאימים על מנת להבטיח שהגישה למידע של Barclays מוגבל לגורמים מורשים (סודיות), שהוא מוגן מפני שינויים בלתי מורשים (שלמות) ושהוא ניתן לאחזר ולהצגה, בהתאם לדרישה (זמינות). אי-יישום של הדרישות עלול לגרום לכך שמידע רגיש של Barclays יהיה פגיע לשינויים בלתי מורשים, לגילוי, לגישה, לנזק, לאובדן או

	יש להחיל אמצעים למניעת זליגת נתונים על מערכות, רשתות וכל מכשיר אחר המשמש לעיבוד, אחסון או העברת נתונים/מידע של Barclays.	להרס, שעשויים להוביל לסנקציות משפטיות ורגולטוריות, לנזק למוניטין, או לאובדן/שיבוש של פעילות עסקית
10. אבטחת נתונים	על הספק לאבטח את הנתונים של Barclays המוחזקים ו/או המעובדים על ידו באמצעות שילוב של הצפנה, הגנת יושרה וטכניקות למניעת אובדן נתונים. יש להגביל את הגישה לנתונים של Barclays לעובדים מורשים בלבד, ולהבטיח הגנה נאותה מפני שיבוש, מתקפות צבירה, מתקפות היסק, איומי אחסון, כולל בין היתר איומים בסביבות של מחשוב ענן. על אמצעי האבטחה לכסות, ללא הגבלה, את התחומים הבאים: 1. על הספק לציית בכל עת לכל החוקים החלים על הגנת נתונים. 2. על הספק ליצור מדיניות, תהליכים ונהלים מספקים תמיכה הולמת בתהליכים עסקיים ובאמצעים טכניים. על הספק להבטיח תיעוד ותחזוקה הולמים של זרימת הנתונים עבור נתונים המאוחסנים במיקום הגאוגרפי של השירות (פיזי ווירטואלי). עליכם לכלול פרטים הקשורים לאפליקציות ולרכיבי מערכות המהווים חלק בלתי נפרד מזרימת הנתונים. 3. על הספק להקפיד לשמר תרשימי זרימה של נתוני Barclays המאוחסנים במיקומים גאוגרפיים (פיזיים ווירטואליים) באפליקציות וברכיבי מערכות. 4. על הספק להקפיד להחזיק במלאי המונה את כל המידע הרגיש/הסודי של Barclays המאוחסן, מעובד או מועבר על ידו. 5. על הספק לוודא שכל הנתונים של Barclays מסווגים ומתויגים בהתאם לתקן סיווג המידע וההגנה המאושר על ידי ההנהלה. 6. הגנה על נתונים במנוחה. א. יש להצפין נתונים במנוחה באופן חזק שימנע חשיפה של נכסי המידע של Barclays 7. מעקב אחר פעילות מסד הנתונים. א. יש לעקוב אחר הגישה והפעילות של מסד הנתונים ולרשום אותן כדי שניתן יהיה לזהות במהירות וביעילות פעילויות זדוניות. 8. הגנה על נתונים בשימוש. א. יש ליישם אמצעי פיקוח לצורכי ניהול הגישה בעת עיבוד מידע רגיש כדי להתגונן מפני פעילויות שייעודן ניצול לרעה של מידע רגיש ב. יש להשתמש בטכנולוגיות הסוואת נתונים כדי להגן באופן יעיל על נתונים רגישים הנמצאים בשימוש מפני גילוי לא מכוון ו/או ניצול זדוני. 9. הגנה על נתונים במעבר. א. יש למנף יכולות הצפנה חזקות כדי להבטיח שנתונים במעבר תמיד מוגנים. ב. ניתן ליישם הצפנה חזקה של נתונים במעבר באמצעות שימוש בהצפנה מסוג Transport או Payload (Message או Selective Field). מנגנוני הצפנת תעבורה כוללים, אך אינם מוגבלים לתחומים הבאים: 10. Transport Layer Security (TLS) (בהתאם לשיטות העבודה הטובות ביותר בתעשייה בתחום קריפטוגרפיה מודרנית, כולל שימוש/דחייה של פרוטוקולים וצופנים) 11. יש להגן על כל הנתונים המאוחסנים בסביבת ייצור ובסביבה שאינה סביבת ייצור באמצעות הצפנה (יש לעיין בסעיף 16: קריפטוגרפיה)	

11. אבטחת תוכנות ואפליקציות	על הספק לפתח אפליקציות באמצעות שימוש בנוהלי קידוד מאובטחים ובסביבה מאובטחת. כשהספק מפתח אפליקציות לשימוש על ידי Barclays או כאלה המשמשות לתמיכה בשירותים המסופקים ל-Barclays, הספק חייב להקים מסגרת לפיתוח תוכנה מאובטחת כדי לשלב אבטחה במחזור החיים של פיתוח התוכנה. על הספק לבדוק ולתקן נקודות תורפה בתוכנה לפני מסירתה ל-Barclays. אבטחת תוכנות ואפליקציות צריכה לכסות, ללא הגבלה, את התחומים הבאים: • הקמה ואימוץ תקני קידוד מאובטח שאושרו על-ידי ההנהלה, בהתאם לשיטות העבודה הטובות ביותר בתעשייה, כדי למנוע פגיעויות והפרעות שירות. • הקמת שיטות קוד מאובטחות המתאימות לשפת התכנות. • כל פיתוח חייב להתבצע בסביבה שאינה סביבת ייצור. • יש להקפיד על סביבות נפרדות עבור מערכות ייצור ומערכות שאינן מערכות ייצור. יש למנוע גישה לא מפוקחת של מפתחים לסביבות ייצור. • יש הפרדה בין החובה לסביבות הייצור ולסביבה שאינה סביבת ייצור. • מערכות מפותחות בהתאם לנוהלי שיטות העבודה הטובות ביותר בתעשייה לפיתוח מאובטח (כגון OWASP). • הקוד צריך להיות מאוחסן בצורה מאובטחת ובכפוף לאבטחת איכות. • אין להעתיק מידע רגיש לסביבות הפיתוח והבדיקה של מערכת, אלא אם יושמו אמצעי פיקוח שווי ערך למערכות הפיתוח והבדיקה. • יש להגן על הקוד מפני שינויים בלתי מורשים לאחר שהבדיקות נחתמו ונמסרו לייצור. • יש להשתמש רק ברכיבי צד שלישי מעודכנים ומהימנים עבור התוכנה שפותחה על-ידי הספק. • יש להחיל כלי ניתוח סטטיים ודינמיים כדי לוודא שמירה על נוהלי קידוד מאובטחים. • הספק חייב להבטיח שנתונים חיים (כולל מידע אישי) לא ישמשו בסביבות שאינן סביבות ייצור. • ממשקי אפליקציות ותכנות (API) יתוכננו, יפותחו, ייפרסו וייבדקו בהתאם לשיטות העבודה הטובות ביותר בתעשייה (כגון OWASP עבור אפליקציות אינטרנט). • אין להשתמש במאגרי קוד ציבורי על הספק להגן על אפליקציות אינטרנט באמצעות פריסת חומות אש של אפליקציות אינטרנט (WAF) הבודקות את כל התעבורה הזורמת אל אפליקציית האינטרנט מפני מתקפות נוכחיות ונפוצות של אפליקציות אינטרנט. עבור אפליקציות שאינן מבוססות אינטרנט, יש לפרוס חומות אש ספציפיות עבור אפליקציות, אם כלים כאלה זמינים עבור סוג האפליקציה הרלוונטי. אם התעבורה מוצפנת, על המכשיר לפעול מאחורי הצפנה או לאפשר פענוח של התעבורה לפני הניתוח. אם אף אחת מהאפשרויות אינה זמינה, יש לפרוס חומת אש עבור אפליקציות אינטרנט מבוססות מארח. על הספק לוודא שכל פתרון 'שירות כתוכנה' (SaaS) מבוסס אינטרנט המבוסס על פתרון אפליקציה המשמש לצורך אספקת השירותים ל-Barclays כולל בקרת גישה משלימה (בקרת אימות) בנוסף לבקרת אימות מסורתית (שם משתמש/סיסמה). על הספק לכלול, ללא הגבלה, את התחומים הבאים: • אימות רב-גורמי (כגון אסימון, הודעת SMS) • כניסה יחידה (SSO) • בקרת גישה מבוססת כתובת IP	אמצעי פיקוח המגנים על פיתוח האפליקציות מסייעים להבטיח כי האפליקציות נותרות מאובטחות גם לאחר פריסתן.

	יש להקצות בקרת גישה משלימה עבור עובדי הספק/קבלני משנה/מעבדי משנה/עובדי Barclays/לקוחות ו/או לקוחות של Barclays.	
12. ניהול גישה לוגית (LAM)	יש להעניק גישה לנכסי מידע (כולל תוכנה, חומרה ונתונים) רק על בסיס 'הצורך לדעת', בהתאם לעקרון של רמת הרשאות מינימלית. הבעלים של נכסי מערכת המידע אחראי לספק רשימה של כל החשבונות שיש להם גישה לנכס המערכת/מידע, כמו גם הגדרת מודל האבטחה של גישה לוגית, כולל גישה פרופילים וכללי הפרדה של תחומי אחריות (SoD). אפליקציות האינטרנט המתארחות של הספק נמצאות בטווח קליטת רשת ה-LAM של Barclays ויש ליישם את אמצעי הפיקוח של רשת ה-LAM של Barclays עבור אפליקציות אלה. • בסיס '**הצורך לדעת**' פירושו שעובדים מקבלים הרשאות גישה למידע הדרוש להם רק כדי לבצע את משימותיהם. למשל, אם עובד פועל אך ורק מול לקוחות בבריטניה, אין כל בסיס 'צורך לדעת' בהקשר למידע הנוגע ללקוחות בארה"ב. • עיקרון **'הרשאות מינימליות'** משמעו שעובדים זקוקים להרשאות הגישה המינימליות שיאפשרו להם לבצע את משימותיהם. למשל, אם עובד נדרש להציג כתובת של לקוח אך אינו נדרש לשנות אותה, עיקרון 'הרשאות מינימליות' יאפשר לו לקבל גישה מסוג 'לקריאה בלבד'. • **הפרדה בין תחומי האחריות** משמעה גישה ליצירת משימות באופן הקובע שגורם יחיד לא יוכל להשלים אותה – כשהמטרה העיקרית היא צמצום רמת הסיכון לפעילויות הונאה. למשל עובד שמבקש ליצור חשבון לא יהיה הגורם שמאשר את הבקשה. יש להגדיר, לתעד ולאכוף תהליכי ניהול גישה בהתאם לשיטות העבודה הטובות ביותר בענף, ובהתאם למדיניות אבטחת הסייבר והמידע של קבוצת Barclays ותקני ניהול הזיהוי והגישה (IAM) במסגרת הפעולות הבאות: • **קליטת LAM של Barclays:** הספק חייב להבטיח שתהליכי ניהול הגישה ימנפו את ערכת הכלים המרכזית של Barclays IAM כדי ליישם אמצעי ביקורת של LAM. יש למסור את רשימות בקרות גישה למערכת ה-IT (ACL) לצוות ה-IAM כחלק מתהליך הקליטה של מערכת ה-IT לערכת הכלים של IAM. כדי לוודא שמתבצעת הפעולה היעילה ביותר של בקרות LAM במורד הזרם, על הספק לוודא שתדירות ההזנה היא הזנה אוטומטית יומית. במערכות שתומכות בגישה ראשית למשתמשים, למשל, Domain/Remote Access, Exchange, ה-ACL חייב להיות יומי. • **פקדי Joiner**: כל גישה מחייבת אישור וסיבה הולמת לפני ביצוע ההקצאה. • **פקדי Mover**: יש לבדוק כל גישה לפני יום ההעברה כדי לאשר את הרשאות הגישה שיש לשמור, לבטל ולהפעיל. יש להסיר את הרשאות הגישה שאושרו לביטול יום לפני ביצוע ההעברה. • **פקדי Lever**: יש להסיר הרשאות שמשמשות לקבלת גישה למשאבי המידע של Barclays ו/או לאספקת השירותים ל-Barclays בתאריך הסיום של החוזה של העובד עם הספק. • **בעלות על החשבון**: חשבון ייחודי חייב להיות משויך לעובד יחיד, שאחראי לכל הפעילות שמבוצעת באמצעות החשבון. אין לשתף פרטי חשבון וסיסמאות עם עובד אחר.	בקרות LAM מתאימות מסייעות להבטיח כי נכסי המידע מוגנים מפני שימוש בלתי הולם. בקרות ניהול גישה מסייעות להבטיח כי רק משתמשים עם הרשאות מתאימות יוכלו לקבל גישה לנכסי המידע.

	• **חשבונות רדומים**: יש להשעות/להשבית חשבונות שאינם בשימוש במשך 60 ימים רצופים לפחות (יש להקפיד על שמירת רשומות מתאימות). • **חידוש הגישה**: כל הרשאת גישה חייבת להיבדק – כל 12 חודשים (עבור גישה ללא הרשאות), וכל 6 חודשים (עבור גישה מועדפת), כדי להבטיח שהרשאת הגישה הולמת. • **אימות זהות (ID&V)**: יש ליישם אמצעי פיקוח מתאימים כדי לוודא שתהליכי ניהול הגישה כוללים מנגנונים לאימות זהות. • **אימות**: יש לאמת את כל החשבונות לפני מתן הרשאת גישה לוגית. אפליקציות ומנגנוני אימות אינם יכולים להציג סיסמאות או מספרי PIN. יש להפעיל אמצעי פיקוח להבטחת אורך ורמת מורכבות נאותים עבור הסיסמה, היסטוריית סיסמאות, תדירות שינוי הסיסמה, אימות רב-גורמי וניהול אישורים מאובטח. • **אבטחת אישורים לא אישיים**: יש לקלוט אישורים לא אישיים (סיסמאות וסודות) בכלי מתאים לניהול אישורים (כגון CyberArk). כשהדבר אפשרי, יש לאבטח את האישורים כדי שאף גורם לא יוכל להשתמש בהם. כשמישהו צריך להשתמש בחשבון, על הגישה להיות זמנית ומוגבלת בזמן ויש לאפס את האישורים לאחר מכן. • **ניהול אישורים**: יש לשנות את הסיסמה של החשבון האישי לפחות כל 90 יום. יש לשנות את הסיסמאות לחשבונות עם עדיפות ולחשבונות אינטראקטיביים כל 120 יום או לאחר כל שימוש אנושי כדי שאף גורם לא ידע את הסיסמה או, אם הסיסמה היא בת 30 תווים ומעלה, כל 365 יום או אחרי כל שימוש אנושי, כדי שאף גורם לא ידע אותה. סיסמאות עבור חשבונות אינטראקטיביים חייבות להיות שונות מ-12 הסיסמאות הקודמות. • **גישה מוגבלת בזמן**: גישה אישית עם הרשאות מיוחדות לתשתית הייצור וסביבת ההתאוששות מאסון, המשמשת את עובדי Barclays או צוות זמני של Barclays, חייבת להיות מוגבלת בזמן, עם אישורים מתאימים. • **ניטור פעילויות בעדיפות:** יש לקיים ניטר אחר פעילויות בעדיפות. הנחיות עבור לקוח שירותי ענן (ספק) המשמשים לצורכי אספקת שירותים ל-Barclays לקוח שירותי הענן (CSC) נדרש לוודא פריסה של בקרות ניהול גישה לוגיות כדי להבטיח את רמת האבטחה של השירותים המסופקים ל-Barclays – • על לקוח שירותי הענן ליישם טכניקות אימות הולמות (כגון אימות רב-גורמי) כדי את זהותם של מנהלי המערכת אצל ספק שירותי הענן ולבצע התאמה ליכולות הניהוליות של ספק שירותי ענן, בהתאם לסיכונים שזוהו. • על לקוח שירותי הענן להבטיח כי ניתן להגביל את הגישה למידע בסביבת שירותי הענן, בהתאם למדיניות בקרת הגישה שיושמה על ידו וכי הגבלות כאלה ישימות ופועלות. הדבר כולל הגבלת הגישה לשירותי הענן, פונקציות שירותי הענן ונתוני לקוחות של שירותי ענן המוחזקים בשירות. • כשמותר להשתמש בתוכניות שירות, על לקוח שירותי הענן לזהות את תוכניות השירות שבהן ניתן להשתמש בסביבת מחשוב הענן שלו ולוודא שהן אינן מפריעות לפעילות התקינה של אמצעי הפיקוח על שירות הענן.	

13. ניהול נקודות תורפה	על הספק להפעיל תוכנית יעילה לניהול נקודות תורפה באמצעות יישום מדיניות ונהלים שנקבעו, תמיכה בתהליכים/אמצעים ארגוניים, אמצעים טכניים, כדי שיוכל לנטר, לזהות ולתקן באופן יעיל ותוך פרק זמן סביר נקודות תורפה באפליקציות שבבעלות הספק או ברכיבי האפליקציות/הקוד, ברשת התשתית וברכיבי מערכת בפיתוח, כדי להבטיח את היעילות של אמצעי האבטחה המיושמים. על ניהול נקודות התורפה לכסות, ללא הגבלה, את התחומים הבאים: • תפקידים מוגדרים, תחומי אחריות ויכולות חשבונאיות לניטור, דיווח, הסלמה ותיקון. • כלים ותשתית מתאימים לביצוע סריקה וזיהוי של נקודות תורפה. • ספק השירות יבצע סריקות לצורכי זיהוי נקודות תורפה על בסיס שגרתי באמצעות חתימות נקודות תורפה מעודכנות (באופן קבוע, כפי שהוכתב במסגרת שיטות העבודה הטובות ביותר בתעשייה), כדי לזהות ביעילות נקודות תורפה ידועות ובלתי ידועות בכל סיווגי הנכסים בסביבה. • עליו להשתמש בתהליך דירוג סיכונים כדי לקבוע סדרי עדיפויות לתיקון נקודות תורפה שזוהו. • עליו לוודא שנקודות התורפה תוקנו ביעילות באמצעות פעולות תיקון חזקות וניהול תיקונים, על מנת להפחית את רמת הסיכון לניצול נקודות תורפה (התיקון יתרחש תוך פרק זמן סביר ובהתאם לשיטות העבודה הטובות ביותר בתעשייה או בהתאם לתוכנת ניהול התיקונים). • עליו ליצור תהליך אימות של תיקון נקודות תורפה המאמת במהירות וביעילות תיקון של נקודות תורפה בכל סוגי הנכסים בסביבה. • עליו לבצע השוואות באופן קבוע בין תוצאות הסריקות שמתרות ומזהות נקודות תורפה כדי לוודא שנקודות התורפה תוקנו תוך פרק זמן סביר. עבור שירותי ספקים הקשורים ל**תשתית אירוח/אפליקציות** של Barclays (כולל **צדדים שלישיים בסיכון גבוה**) • על הספק להודיע ל-Barclays באופן מיידי בכל מקרה של זיהוי נקודות תורפה קריטיות. • על הספק לתקן נקודות תורפה בהתאם לטבלה שלהלן או בהתאם להנחיות של Barclays (צוות TPSecM במשרד סמנכ"ל האבטחה).	אי יישום אמצעי פיקוח זה עלול להוביל לניצול נקודות תורפה על ידי פורצים תוך ביצוע מתקפות סייבר שעלולות להוביל לנזק רגולטורי ו/או לפגיעה במוניטין.

עדיפות	דירוג	ימי סגירה (מקסימום)
P1	קריטי	15 (30 ימים לכל היותר)
P2	גבוה	60
P3	בינוני	180
P4	חלשה	אין SLA

	יש להודיע ל-Barclays באופן מיידי על כל בעיות האבטחה ונקודות התורפה שעלולות להיות בעלות השפעה מהותית על תשתית האירוח של Barclays או על אפליקציות שסופקו על ידי הספק, כשהספק החליט ליטול (צוות TPSecM במשרד סמנכ"ל האבטחה, בכתובת externalcyberassurance@barclayscorp.com). **הנחיות עבור לקוח שירותי ענן (ספק) המשמשים לצורכי אספקת שירותים ל-Barclays** לקוח שירותי הענן (CSC) נדרש לוודא פריסה של בקרות ניהול נקודות תורפה נאותות כדי להבטיח את רמת האבטחה של השירותים המסופקים ל-Barclays – • על לקוח שירותי הענן לבקש מידע מספק שירותי הענן על ניהול פרצות טכניות שעלולות להשפיע על שירותי הענן המסופקים. על לקוח שירותי הענן לזהות את נקודות החולשה הטכניות שהוא יהיה אחראי לנהל ולאחר מכן להגדיר תהליך ניהול הולם.	
14. ניהול טלאי תיקון	על הספק להשתמש בתוכנה לניהול תיקונים שנתמכת על-ידי מדיניות ונהלים שנקבעו, תהליכים עסקיים/אמצעים ארגוניים ולהפעיל אמצעים טכניים כדי לפקח/לעקוב אחר הצורך בתיקון ופריסה של תיקוני אבטחה על מנת לנהל את כל סביבת הספקים/הנכסים. הספק חייב להבטיח ששרתים, התקני רשת, אפליקציות והתקני נקודת קצה יקבלו את עדכוני האבטחה העדכניים ביותר ובהתאם לשיטות העבודה הטובות ביותר בתעשייה על מנת להבטיח כי: • הספק יעריך ויבדוק את כל התיקונים במערכות המייצגות במדויק את התצורה של מערכות ייצור היעד לפני פריסת התיקון במערכות הייצור וכי הפעולה הנכונה של השירות המתוקן מאומתת לאחר כל פעילות תיקון. אם לא ניתן לתקן את המערכת, יש לפרוס אמצעי נגד מתאימים. • יש לרשום, לבדוק ולאשר את כל השינויים העיקריים במערכת ה-IT לפני היישום באמצעות תהליך ניהול שינויים מאושר וחזק, כדי לתמוך בדרישות עתידיות של ביקורת, חקירה, פתרון בעיות וניתוח. • על הספק לוודא שתיקונים משתקפים בסביבות ייצור והתאוששות מאסון (DR).	אם פקד זה לא יישום, שירותים עשויים להיות פגיעים לבעיות אבטחה שעלולות לפגוע בנתוני הצרכנים, לגרום לאובדן שירות או לאפשר פעילות זדונית אחרת.
15. בדיקת חדירה/הערכה של מערך אבטחת ה-IT	הספק חייב ליצור קשר עם ספק שירותי אבטחה מוסמך ועצמאי כדי לבצע הערכת אבטחת IT/בדיקת חדירה המכסה את כלל תשתית ה-IT, כולל אתר התאוששות מאסון ואפליקציות אינטרנט הקשורים לשירותים שהספק מספק ל-Barclays. יש לנקוט פעולה זו לפחות מדי שנה כדי לזהות נקודות תורפה הניתנות לניצול ועלולות להוות אזורים שדרכם תיפרץ מסגרת האבטחה על הנתונים של Barclays באמצעות יישום מתקפות סייבר. יש להעניק עדיפות לכל נקודות התורפה ולעקוב אחר התקדמותן עד לפתרון. יש לבצע את הבדיקה בהתאם לשיטות העבודה הטובות ביותר בתעשייה. עבור שירותי ספקים הקשורים ל**תשתית אירוח/אפליקציות** של Barclays (כולל **צדדים שלישיים בסיכון גבוה**) • על הספק להודיע לאנשי צוות ה-TPSecM ולהסכים איתם על היקף הערכת האבטחה עם Barclays, במיוחד תאריך/שעת ההתחלה והסיום, כדי למנוע הפרעה לפעילות השוטפת של Barclays.	אם אמצעי פיקוח זה לא יישום, ייתכן שהספק לא יוכל להעריך את איומי הסייבר שעמו עליו להתמודד ואת רמת התאימות והחוזר של אמצעי ההגנה שהוא מיישם. מידע של Barclays עשוי להיחשף ואף עלולים להתרחש חשיפה ו/או אובדן שירות שיובילו לנזק רגולטורי או לפגיעה במוניטין.

<table>
<tr>
<td></td>
<td>

יש ליצור קשר עם Barclays (צוות TPSecM במשרד סמנכ"ל האבטחה) כדי לדון על הנושאים שמוסכם שיש בהם סיכון.
על הספק לשתף את דוח הערכת האבטחה העדכני על בסיס שנתי עם Barclays (צוות TPSecM במשרד סמנכ"ל האבטחה בכתובת externalcyberassurance@barclayscorp.com)
על ספק להודיע ל-Barclays באופן מיידי בכל מקרה של זיהוי נקודות תורפה קריטיות.
על הספק לתקן נקודות תורפה בהתאם לטבלה שלהלן או בהתאם להסכם עם Barclays (צוות TPSecM במשרד סמנכ"ל האבטחה).

<table>
<tr><th>עדיפות</th><th>דירוג</th><th>ימי סגירה (מקסימום)</th></tr>
<tr><td>P1</td><td>קריטי</td><td>15 (30 ימים לכל היותר)</td></tr>
<tr><td>P2</td><td>גבוה</td><td>60</td></tr>
<tr><td>P3</td><td>בינוני</td><td>180</td></tr>
<tr><td>P4</td><td>חלשה</td><td>אין SLA</td></tr>
</table>
</td>
<td></td>
</tr>
<tr>
<td>16. קריפטוגרפיה</td>
<td>
הספק חייב לוודא שמתבצע שימוש נכון ויעיל בקריפטוגרפיה כדי להגן על הסודיות, האותנטיות או השלמות של הנתונים/המידע של Barclays בהתאם לדרישות העסקיות ואבטחת המידע ולהתחשב בדרישות חוקיות, סטטוטוריות, רגולטוריות וחוזיות שקשורות לקריפטוגרפיה.

בעת שימוש בקריפטוגרפיה, יש לשקול את הדברים הבאים:

המדיניות הספציפית לנושא הקריפטוגרפיה המוגדרת על ידי הארגון, כולל העקרונות הכלליים להגנה על מידע. מדיניות ספציפית לנושא על השימוש בקריפטוגרפיה – יש להגדיל את היתרונות ולצמצם את הסיכונים של השימוש בטכניקות קריפטוגרפיות כדי למנוע שימוש לא מתאים או שגוי.
זיהוי רמת ההגנה הנדרשת וסיווג המידע וכתוצאה מכך קביעת סוג, חוזק ואיכות האלגוריתמים הקריפטוגרפיים הנדרשים.
השימוש בקריפטוגרפיה להגנה על מידע המוחזק בהתקן אחסון ומועבר דרך רשתות למכשירים או למדיה לאחסון.
הגישה לניהול מפתחות, כולל שיטות להתמודד עם הדור ושיטת ההגנה של מפתחות קריפטוגרפיים, כמו גם שחזור של מידע מוצפן במקרה של אובדן, פגיעה או נזק למפתחות.
רציונל קריפטוגרפיה – הספק חייב לתעד את הרציונל לשימוש בטכנולוגיה קריפטוגרפית ולסקור זאת כדי לוודא שהיא עדיין מתאימה למטרה.
הליכי מחזור חיים של קריפטוגרפיה – הספק חייב להחזיק ולתחזק קבוצה מתועדת של הליכי ניהול מחזור חיים של קריפטוגרפיה המפרטים את התהליכים מקצה לקצה לניהול מפתחות

</td>
<td>הגנה עדכנית ואלגוריתמים מתאימים להצפנה מבטיחים הגנה רצופה על נכסי המידע של Barclays.</td>
</tr>
</table>

		מדור, טעינה, הפצה להרס. על הספק להוציא את המפתחות מפעילות לאחר תום תקופת השירות או להגדיר תוכנת חובה לסיבוב מפתחות. • אישורים דיגיטליים – הספק חייב להבטיח שכל האישורים מתקבלים מתוך קבוצה של רשויות אישורים (CA) מאושרות ומאומתות שיש להן שירותי ביטול ומדיניות ניהול אישורים וחייבות להבטיח שאישורים שנחתמו בעצמם ינוצלו רק כאשר מבחינה טכנית לא ניתן לתמוך בפתרון מבוסס CA וחייבים להיות בקרות ידניות במקום כדי להבטיח את השלמות, האותנטיות של המפתחות ואת הביטול והחידוש בזמן. • אישור פעולות ידניות – הספק חייב להבטיח שכל האירועים המנוהלים על ידי בני אדם עבור מפתחות ואישורים דיגיטליים, כולל רישום ויצירת מפתחות ואישורים חדשים, יאושרו ברמה המתאימה ורשומה של האישור נשמרת. • יצירת מפתח ותקופת קריפטוגרפיה – הספק חייב להבטיח כי כל המפתחות מופקים באופן אקראי על ידי חומרה מאושרת או הצפנה מאובטח Pseudo Random Number Generator (CSPRNG) בתוכנה. ○ הספק חייב להבטיח שכל המפתחות יהיו כפופים למחזור חיים מוגבל ומוגדר של תקופת הקריפטוגרפיה, עד למועד שבו הם יוחלפו או יושבתו. הדבר חייב להתבצע בהתאם לדרישות המכון הלאומי לתקנים וטכנולוגיה (NIST) ולשיטות העבודה הטובות ביותר בתעשייה. • הגנת על אחסון מרכזי – הספק חייב להבטיח שמפתחות קריפטוגרפיים סודיים/פרטיים קיימים רק בתצורות הבאות: ○ בגבול הקריפטוגרפי של התקן/מודול אבטחה עם חומרה מאושרת. ○ באופן מוצפן במסגרת מפתח קיים או מבוסס סיסמה אחר. ○ בחלקים מפוצלים המחולקים בין קבוצות אפוטרופסות נפרדות. ○ יש לנקות את זיכרון המארח למשך תקופת הפעולה הקריפטוגרפית, אלא אם נדרשת הגנת HSM. • הספק חייב להבטיח שמפתחות נוצרים ומוחזקים בגבולות הזיכרון של HSM עבור מפתחות ברמת סיכון גבוהה. זה כולל: ○ מפתחות עבור שירותים מוסדרים שבהם HSM היא דרישת חובה. ○ אישורים המייצגים את Barclays מ-CA ציבורי. ○ אישורי Root, Issuing, OCSP ו-RA (רשות רישום) המשמשים להנפקת אישורים המגנים על שירותי Barclays. ○ מפתחות המגנים על מאגרי אחסון נצברים של מפתחות, אישורי אימות או נתוני PII. • גיבוי ואחסון מרכזיים – הספק שומר על גיבוי של כל המפתחות כדי למנוע את הפסקת השירות אם המפתחות פגומים או דורשים שחזור. הגישה לגיבוי מוגבלת למיקומים מאובטחים תחת ידע מפוצל ובקרה כפולה. גיבויי מפתח חייבים להיות בעלי הגנה קריפטוגרפית חזקה לפחות כמו המפתחות הנמצאים בשימוש. • מלאי – הספק שומר על מלאי מלא ועדכני של שימוש קריפטוגרפי במסגרת השירותים שהוא מספק ל-Barclays, המפרט את כל המפתחות הקריפטוגרפיים, האישורים הדיגיטליים, תוכנת ההצפנה וחומרה קריפטוגרפית המנוהלת על ידי הספק כדי למנוע נזק במקרה של תקלה. עדות לכך היא חתימת המלאי שנבדק לפחות בכל רבעון ומסירתו ל-Barclays. המלאי חייב לכלול (כשרלוונטי):	

	○ צוות תמיכת IT ○ נכסים קשורים ○ אלגוריתמים, אורך המפתח, סביבה, היררכיית מפתח, רשות אישורים, טביעת אצבע, הגנת מפתח לאחסון ומטרה טכנית ותפעולית. • מטרה פונקציונלית ותפעולית - המפתחות חייבים להיות בעלי מטרה תפקודית ותפעולית אחת ולא להיות משותפים בין שירותים מרובים או מעבר לשירותים של Barclays. • נתיבי ביקורת – על הספק לבצע ולשמור ראיות לסקירת רשומות שניתנות לביקורת בכל רבעון לכל הפחות עבור כל אירועי ניהול מחזור החיים של המפתח ושל האישורים המדגימים שרשרת משמורת מלאה לכל המפתחות, כולל יצירה, הפצה, טעינה והרס, כדי לזהות שימוש בלתי מורשה. • חומרה – הספק מאחסן את התקני החומרה באזורים מאובטחים ושומר על נתיב ביקורת לאורך מחזור החיים של המפתח כדי להבטיח ששרשרת המשמורת על התקנים קריפטוגרפיים לא תיפגע. נתיב זה נבדק על בסיס רבעוני. • הספק חייב לוודא שחומרה קריפטוגרפית מאושרת לפחות לרמה של FIPS140-2 Level 2 ולהגיע לרמה 3 של אבטחה פיזית וניהול מפתחות קריפטוגרפיים או PCI HSM. הספק רשאי לבחור לאפשר כרטיסים חכמים מבוססי שבב או אסימונים אלקטרוניים מאושרים על ידי FIPS כחומרה מקובלת לאחסון מפתחות המייצגים ומוחזקים על ידי אנשים או לקוחות בודדים כאשר הם מוחזקים מחוץ לאתר. • מפתח בסיכון – הספק שומר ומנטר תוכנית מפתחות בסיכון כדי להבטיח שמפתחות חלופיים נוצרים ללא תלות במפתח הפגוע, כדי למנוע מהמפתח הפגוע לספק כל מידע בנוגע להחלפתו. במקרה של תקרית כלשהי, יש ליידע את Barclays: **המרכז למבצעים משותפים (JOC) במשרד סמנכ"ל האבטחה בכתובת gcsojoc@barclays.com** • חוזק האלגוריתמים והמפתחות – הספק מבטיח את הסרת האלגוריתמים החלשים ושהאלגוריתמים ואורך המפתחות שנמצאים בשימוש תואמים לדרישות המכון הלאומי לתקנים וטכנולוגיה (NIST) ולשיטות העבודה הטובות ביותר בענף. • על הספק להעריך את השימוש באלגוריתמים קוונטיים פגיעים ובתוכניות העברה שיש לטפל בהן.	
17. מחשוב ענן	ספק שירותי הענן (CSC) חייב להבטיח ששירות הענן המשמש עבור שירותי Barclays כולל מסגרת בקרות אבטחה מוגדרת היטב כדי לעמוד ביעדי הסודיות, השלמות והזמינות ועל מנת להבטיח כי בקרות האבטחה קיימות ופועלות ביעילות ומגנות על השירותים של Barclays. על הספק להחזיק בהסמכה לתקן ISO/IEC 27017 או 27001 או SOC 2 או במסגרת אבטחת ענן דומה או ליישם את שיטות העבודה הטובות ביותר בתעשייה כדי ליישם אמצעי אבטחה מבוססים ולהבטיח שכל השימוש בטכנולוגיית ענן מאובטח. יש לוודא שספק שירותי הענן מוסמך לשיטת העבודה הטובות ביותר בתעשייה, לרבות יישום אמצעי פיקוח מתאימים המקבילים לגרסה העדכנית ביותר של Cloud Security Alliance, Cloud Controls Matrix (CCM).	אם אמצעי פיקוח זה לא יושם, הנתונים של Barclays עלולים להיפגע והתוצאה היא נזק רגולטורי ו/או פגיעה במוניטין.

	הספק אחראי להבטיח בקרות אבטחת מידע הקשורות לנכסי מידע/נתונים של Barclays, כולל מידע אישי בתוך הענן וספק שירותי הענן CSP אחראי על אבטחת סביבת מחשוב הענן. הספק נותר אחראי על הגדרת התצורה והניטור של יישום בקרות אבטחה כדי להגן מפני כל אירועי אבטחה, כולל הפרות נתונים. על הספק ליישם אמצעי אבטחה בכל ההיבטים של השירות המסופק, כולל מודל האחריות המשותפת בענן, כך שהוא מגן על הסודיות, השלמות, הזמינות והנגישות על-ידי מזעור ההזדמנות של גורמים בלתי מורשים לקבל גישה למידע של Barclays ולשירותים ש-Barclays משתמשת בהם. אמצעי פיקוח על אבטחת הענן צריכות לכסות, אך אינם מוגבלים לתחומים הבאים עבור מודלי הפריסה (IaaS/PaaS/SaaS): • מנגנוני פיקוח ואחריות • ניהול זהויות וגישה • אבטחת רשת (כולל קישוריות) • אבטחת נתונים (במעבר/במנוחה/באחסון) • מחיקת נתונים/ניקוי נתונים מאובטח • קריפטוגרפיה, הצפנה וניהול מפתחות – CEK • רישום וניטור • וירטואליזצייה • הפרדת שירותים נכסי המידע/הנתונים של Barclays, לרבות מידע אישי שמאוחסן בענן כחלק מהשירותים של Barclays, חייבים לקבל אישור של Barclays (צוות TPSecM במשרד סמנכ"ל האבטחה). הספק ימסור ל-Barclays מידע לגבי מיקומם של אזורי הנתונים ואזורי נתונים של מעבר לגיבוי בעת כשל שבהם הנתונים של Barclays יאוחסנו.	

חלל בנק ייעודי(BDS)

מיועד עבור שירותים שמחייבים מרחב בנק ייעודי (BDS) ורשמי, יש צורך בדרישות פיזיות וטכניות ספציפיות של BDS. (אם BDS הוא דרישה לשירות, דרישות הפיקוח יהיו ישימות).

סוגי BDS השונים הם:

Tier 1 (First class) – כל תשתית ה-IT מנוהלת על ידי **Barclays** באמצעות הקצאת התקני LAN, WAN ו-Desktop המנוהלים על ידי **Barclays** לאתר של ספק עם מרחב ייעוד המיועד עבור השירותים המסופקים ל-Barclays.

Tier 2 (Business Class) – כל תשתית ה-IT מנוהלת על ידי **הספק** ומתחברת לשערי Extranet של **Barclays** – התקני LAN, WAN ו-Desktop נמצאים בבעלות הספק ומנוהלים על ידו.

Tier 3 (Economy class) – כל תשתית ה-IT מנוהלת על ידי **הספק** ומתחברת לשערי האינטרנט של **Barclays** – התקני LAN, WAN ו-Desktop נמצאים בבעלות הספק ומנוהלים על ידו

BDS 18.1 – הפרדה פיזית	השטח הפיזי המאוכלס חייב להיות מוקדש לפעילויות הקשורות ל-Barclays ואין לשתפו עם חברות/ספקים אחרים. עליו להיות מופרד באופן הגיוני ופיזי.
BDS 18.2 – בקרת גישה פיזית	• הספק חייב ליישם בעל תהליך גישה פיזי המכסה שיטות גישה ואישור ל-BDS בעת אספקת השירותים. • כניסה ויציאה לאזורי BDS חייבת להיות מוסדרת ומנוטרת על ידי מנגנוני בקרת גישה פיזית כדי להבטיח שרק עובד מורשה יוכל לקבל גישה (ספציפית לתפקיד) ויאושר (על ידי בעל שירות ה-BDS). • כרטיס גישה אלקטרוני המאפשר גישה מורשית לאזורי BDS במבנה. • הספק חייב לבצע בדיקה רבעונית כדי להבטיח שרק גורמים מורשים מקבלים גישה ל-BDS. חריגות ייבדקו באופן ייסודי כדי לפתור את הבעיה. • זכויות הגישה מוסרות בתוך 24 שעות לעוזבים, למובילים ולעובדים שאינם מועסקים עוד (הרשומות המתאימות יישמרו). • יש להפעיל אמצעי אבטחה פיזיים (שומרים אנושיים) שיסיירו באופן שגרתי באזור BDS כדי לזהות ביעילות גישה לא מורשית או פעילות זדונית אפשרית • יש להפעיל אמצעי אבטחה אוטומטיים לצורכי הענקת הרשאות גישה ל-BDS, כולל: לעובד מורשה: ○ תג זיהוי תמונה הגלוי בכל עת ○ הפעלת קוראי קרבה (כרטיסים) ○ מנגנון Anti-Pass Back מופעל ומנוטר • הספק חייב ליישם תהליכים ונהלים לבקרה וניטור של גורמים חיצוניים, לרבות קבלני משנה, מעבדי משנה עם גישה פיזית לאזורי BDS לצורכי תחזוקה וניקיון.
BDS 18.3 – מעקב וידאו	• יישום מעקב וידאו לאזורי BDS כדי להקליט או להתריע ביעילות בשל גישה בלתי מורשית ו/או פעילות זדונית וסיוע בחקירות. • בכל נקודות הכניסה והיציאה של אזור BDS יתבצע מעקב וידאו. • יש לבצע בדיקות של רמת התפעול והאיכות של מצלמות האבטחה כדי לוודא שהן מותקנות כהלכה ומספקות פלט ברור המאפשר זיהוי בכל עת כדי של פעילות זדונית על מנת לסייע בפעילויות חקירה. הספק חייב לאחסן את צילומי מצלמות האבטחה למשך 30 יום, כשכל ההקלטות והמקלטים של מצלמות האבטחה חייבים להיות מאובטחים כדי למנוע שינוי, מחיקה או צפייה 'מזדמנת' בכל אחד ממסכי מערכת מצלמות האבטחה הקשורים, כשהגישה להקלטות חייבת להיות מבוקרת ומוגבלת לגורמים מורשים בלבד.
BDS 18.4 – גישה לרשת של Barclays ולאסימוני אימות של Barclays	• כל משתמש חייב לבצע אימות ברשת של Barclays רק מ-BDS, תוך שימוש באסימון אימות רב-גורמי של Barclays. • על הספק לשמור רשומות של גורמים שלהם סופקו אסימוני אימות של Barclays (אסימוני RSA) ולבצע התאמות רבעוניות. • Barclays תבטל אישורי אימות לאחר הודעה כי אין עוד צורך בהרשאת גישה (למשל, סיום העסקה, הקצאה מחדש של פרויקט וכו') **תאריך יציאה/יום העבודה האחרון/תאריך LDIO שהתקבל** אצל הספק. • Barclays תשבית באופן מיידי אישורי אימות לאחר אי שימוש לפרק זמן מסוים באישורים כגון אלה (תקופת אי השימוש לא תעלה על חודש אחד). • על שירותים עם גישה להדפסה מרחוק באמצעות אפליקציית Barclays Citrix לקבל אישור של Barclays (צוות TPSecM במשרד סמנכ"ל האבטחה). על הספק להחזיק רשומות ולבצע התאמה על בסיס רבעוני. יש לעיין באמצעי פיקוח – 4. עבודה מרחוק (גישה מרחוק)

BDS 18.5 – תמיכה מעבודה חוץ למשרד	גישה מרחוק לסביבת BDS אינה מסופקת כברירת מחדל עבור עבודה שאינה מתבצעת בשעות המשרד/בשעות העבודה/בעת מתן תמיכה מהבית. בכל גישה מרחוק יש לקבל אישור מהצוות הרלוונטי של Barclays (כולל צוות TPSecM במשרד סמנכ"ל האבטחה). אין ליישם מסגרות עבודה מרחוק (כולל עבודה מהבית) במהלך פעילות עסקית רגילה, כשצדדים שלישיים נדרשים על פי חוזה לספק שירותים ממיקום ייעודי של הבנק או ממיקום ייעודי של ספק או כשחלות דרישות רגולטוריות. עם זאת, הוראה כגון זו מותרת במסגרת תוכניות המשכיות עסקית של צדדים שלישיים במקרה של התאוששות מאסון/משבר/תגובה מגפה בהסכמה של Barclays ובהתאם לכל דרישות האבטחה המחייבות המהוות חלק בלתי נפרד מההסכם החוזי, בהקשר של עבודה מרחוק.
BDS 18.6 – אבטחת רשת	• שמירה על מלאי מעודכן של כל גבולות הרשת של הארגון (באמצעות ארכיטקטורת רשת/דיאגרמה). • יש לבדוק את התכנון והיישום של הרשת לפחות מדי שנה. • יש להקפיד על הפרדת רשת BDS מבחינה לוגית מהרשת הארגונית של הספק באמצעות חומת אש, כדי לוודא שכל התעבורה הנכנסת והיוצאת תוגבל ותנוטר. • על תצורת הניתוב להבטיח חיבורים לרשת של Barclays בלבד ואין לנתב אותה לרשתות אחרות של הספק. • יש להגדיר את נתב ה-Edge של הספק, שמתחבר לשער Extranet של Barclays, תוך יישום תפיסה של הגבלת הפיקוח ביציאות, בפרוטוקולים ובשירותים. ○ יש לוודא שפונקציות הרישום והניטור הופעלו. • יש לנטר את רשת ה-BDS ולוודא שרק מכשירים מורשים יקבלו גישה באמצעות יישום אמצעי פיקוח רשת מתאימים יש לעיין באמצעי פיקוח – 2. אבטחת גבולות ורשת
BDS 18.7 – רשת אלחוטית	יש לנטרל אפשרויות לשימוש ברשת אלחוטית עבור רשת BDS בעת אספקת שירותים ל-Barclays.
BDS 18.8 – אבטחת נקודות קצה	יש לאבטח את תצורת ה-Built של מחשבים שולחניים (כולל מחשבים ניידים) בהתאם לשיטות העבודה הטובות ביותר בתעשייה עבור מחשבים ברשת BDS. יש ליישם את שיטות העבודה הטובות ביותר בתעשייה עבור BDS ולוודא שהתקני האבטחה בנקודות הקצה כוללים, אך אינם מוגבלים לתחומים הבאים: • הצפנה מלאה של כונני דיסק קשיח. • השבתת כל התוכנות/השירותים/היציאות שאינם נחוצים. • השבתת זכויות גישה מנהליות עבור משתמשים מקומיים. • עובדי הספק לא יורשו לשנות הגדרות בסיסיות כגון ערכות טיפול המהוות ברירת מחדל, חלוקה למחיצות במערכת, שירותי ברירת מחדל וכו'. • השבתת יציאות USB לצורכי העתקת מידע/נתונים של Barclays לכונני מדיה ניידים • הקפדה על עדכון פתרונות למניעת תוכנות זדוניות לגרסאות העדכניות ביותר והתקנת כל טלאי האבטחה הדרושים. • השבתת האפשרות לבצע הדפסה ברקע • השבתת פונקציות השיתוף/ההעברה של נכסי מידע/נתונים של Barclays באמצעות כלים/תוכנות להעברת הודעות מידיות. • זיהוי, עצירה ותיקון נוכחות ו/או שימוש בתוכנות בלתי מורשות, לרבות תוכנות זדוניות.

	• נעילת אפשרות לפסקי זמן של מסכים, הגבלת חיבורי TCP IP לרשת הארגונית בלבד, יישום סוכני אבטחת EPS מתקדמים לצורכי זיהוי דפוסי התנהגות חשודים. יש לעיין באמצעי פיקוח – 8. אבטחת נקודות קצה
BDS 18.9 – דואר אלקטרוני ואינטרנט	• יש להגדיר באופן מאובטח את קישוריות הרשת כדי שתגביל את פעילות הדואר האלקטרוני והאינטרנט ברשת BDS. • הספק חייב להגביל את היכולת לגשת לאתרי רשתות חברתיות, שירותי דואר אלקטרוני ואתרים עם היכולת לאחסן מידע באינטרנט, כגון Google Drive, Dropbox, iCloud. • על כל העברה לא מורשית של נתוני Barclays מחוץ לרשת BDS להיות מוגנת מפני זליגת נתונים: • כתובת דוא\"ל • אינטרנט/שער אינטרנט (כולל אחסון מקוון ודואר באינטרנט) • יש לאכוף מסנני כתובות URL מבוססי רשת, המגבילים את יכולת המערכת להתחבר רק לאתרי אינטרנט פנים ארגוניים או לאתרי אינטרנט של ארגון הספק בלבד • יש לחסום את כל הקבצים המצורפים ו/או את תכונת ההעלאות לאתרי אינטרנט. • יש לוודא שרק דפדפני אינטרנט ולקוחות דואר אלקטרוני נתמכים באופן מלא מותרים.
BDS 18.10 – מכשיר אישי/BYOD	**אין לאפשר למכשירים אישיים/BYOD לקבל גישה לסביבה של Barclays ו/או לנתונים של Barclays**

הזכות לבדיקה

הספק חייב לאפשר ל-Barclays, לאחר מתן הודעה בכתב לא פחות מעשרה (10) ימי עסקים, לערוך בדיקת אבטחה של כל אתר או טכנולוגיה המשמשים את הספק או את קבלני המשנה/מעבדי המשנה שלו כדי לפתח, לבדוק, לשפר, לתחזק או להפעיל את מערכות הספק המשמשות בשירותים, על מנת לבחון את רמת עמידתו של הספק בהתחייבויותיו כלפי Barclays. כמו כן, על הספק לאפשר ל-Barclays לבצע בדיקה על בסיס שנתי לפחות ו/או מיד לאחר תקרית אבטחה.

כל אי התאמה לבקרות שזוהתה על ידי Barclays במהלך ביצוע הבדיקה חייב להיות סיכון שהוערך על ידי Barclays ו-Barclays חייבת לציין מסגרת זמן לביצוע התיקון הנדרש. לאחר מכן, על הספק להשלים כל תיקון נדרש במסגרת זמן זו.

הספק חייב לספק את כל הסיוע המבוקש באופן סביר על ידי Barclays ביחס לכל בדיקה ותיעוד שנמסרו לו במהלך ביצוע הבדיקה. יש להשלים את התיעוד ולהחזיר אותו מיד ל-Barclays. הספק גם חייב לספק תמיכה ל-Barclays ולמלא את שאלון ההערכה שיכלול את כל הראיות הנדרשות במהלך כל ביצוע של הערכה. על כל צד לשאת בעלויות משלו בהתאם לבדיקות/לביקורות/להערכות.

נספח א': מילון מונחים

הגדרות	
חשבון	קבוצה של אישורים (למשל, מזהה משתמש וסיסמה) המאפשרים גישה למערכת IT מנוהלת באמצעות בקרות גישה לוגיות.
גיבוי	גיבוי או תהליך גיבוי, מתייחס להפקת עותקים של נתונים, כך שניתן יהיה להשתמש בהם כדי לשחזר את המקור לאחר תקרית של אובדן נתונים.
חלל בנק ייעודי	חלל בנק ייעודי (BDS) פירושו כל מקום הנמצא בבעלותו או בשליטתו של חבר בקבוצת הספק או כל קבלן/מעבד משנה, המיועדים באופן בלעדי לפעילות הקשורה ל-Barclays וממנו השירותים מבוצעים או מועברים.
שיטות העבודה הטובות ביותר בתעשייה	שימוש בשיטות עבודה, תהליכים, תקנים ואישורים מובילים בשוק הטובים ביותר והנוכחיים; כמו גם מימוש מידת המיומנות והטיפול, אשר צפוי באופן סביר מארגון מקצועי מיומן, מנוסה ומוביל בשוק, העוסק במתן שירותים זהים או דומים לשירותים המסופקים ל-Barclays.
BYOD	הביאו מכשירים משלכם
קריפטוגרפיה	יישום של תיאוריה מתמטית לפיתוח טכניקות ואלגוריתמים שניתן ליישם על נתונים כדי להבטיח מטרות כגון סודיות, שלמות ו/או אימות נתונים.
אבטחת סייבר	יישום טכנולוגיות, תהליכים, אמצעי פיקוח ואמצעים ארגוניים כדי להגן על מערכות מחשב, רשתות, תוכנית, התקנים ונתונים מפני מתקפות דיגיטליות שעשויות לכלול (אך ללא הגבלה), גילוי בלתי מורשה, הרס, אובדן, שינוי, גנבה או נזק לחומרה, לתוכנה או לנתונים.
נתונים	תיעוד של עובדות, מושגים או הוראות על אמצעי אחסון לתקשורת, אחזור ועיבוד באמצעים אוטומטיים והצגה כמידע המובן על ידי בני אדם.
מניעת שירות (מתקפה)	ניסיון להפוך משאב מחשב ללא זמין עבור המשתמשים שעבורם הוא מיועד.
השמדה/מחיקה	פעולת ההחלפה, המחיקה או ההשמדה הפיזית של מידע, כך שלא ניתן יהיה להשתמש בו.
TPSecM	אחריות צוות ניהול האבטחה של צד שלישי לניהול מערך האבטחה של הספקים.
הצפנה	טרנספורמציה של הודעה (נתונים, קול או וידאו) לצורה חסרת משמעות שלא תובן על ידי קוראים לא מורשים. טרנספורמציה זו מהווה מעבר מתבנית של טקסט רגיל לתבנית של טקסט מוצפן.
HSM	מודול אבטחת חומרה. התקן ייעודי שמספק יצירת מפתח קריפטוגרפי מאובטח, אחסון ושימוש, כולל האצה של תהליכים קריפטוגרפיים.
נכס מידע	כל מידע בעל ערך, בהתחשב בדרישות הסודיות, השלמות והזמינות שלו. או כל פיסת מידע או קיבוץ רכיבי מידע שונים שיש להם ערך עבור הארגון.
בעלי נכס מידע	אדם בתוך הארגון האחראי על סיווג הנכס ועל הבטחת הטיפול הראוי בו.
הרשאות מינימליות	הרמה המינימלית של גישה/הרשאות המאפשרת למשתמש או לחשבון לבצע את תפקידו העסקי.
ציוד רשת/התקן רשת	התקני IT שמחוברים לרשת ומשמשים לניהול, לתמיכה או לשליטה ברשת. יכול לכלול, אך אינו מוגבל לנתבים, מתגים, חומות אש, מאזני עומסים.
קוד זדוני	תוכנה שנכתבה מתוך כוונה לעקוף את מדיניות האבטחה של מערכת IT, מכשיר או יישום. דוגמאות לכך הן וירוסים, סוסים טרויאניים ותולעים.
אימות רב-גורמי (MFA)	אימות המחייב שתי טכניקות אימות שונות או יותר. דוגמה אחת היא השימוש באסימון אבטחה, שבו אימות מוצלח מסתמך על משהו שהאדם מחזיק (כלומר, אסימון האבטחה) ומשהו שהמשתמש יודע (כלומר, קוד הזיהוי האישי של אסימון האבטחה).
פרטים אישיים	כל מידע המשמש לזיהויו של אדם, הן במישרין והן בעקיפין, במיוחד באמצעות הפניה לאמצעים מזהים כגון שם, מספר מזהה, פרטי מיקום, מזהה מקוון או הפניה לגורם אחד או יותר הספציפיים לנתונים פיזיים, פיזיולוגיים, גנטיים, נפשיים, כלכליים, תרבותיים או חברתיים של אותו אדם.
גישה מועדפת	הקצאת גישה, הרשאות או יכולות מיוחדות (מעל הרגיל) למשתמש, לתהליך או למחשב.
חשבון מועדף	חשבון עם רמת שליטה גבוהה יותר במערכת IT ספציפית. חשבונות אלה משמשים בדרך כלל לתחזוקת המערכת, לניהול האבטחה או לביצוע שינויי תצורה במערכות IT. דוגמאות לכך הן חשבון מנהל מערכת, חשבון root, חשבונות Unix עם uid=0, חשבונות תמיכה, חשבונות ניהול אבטחה, חשבונות ניהול מערכת וחשבונות מנהל מערכת מקומיים

גישה מרחוק	טכנולוגיה וטכניקות המשמשות כדי להעניק למשתמשים מורשים גישה לרשתות ולמערכות של הארגון ממיקום מחוץ לאתר.
מערכת	מערכת, בהקשר של מסמך זה, היא אנשים, נהלים, ציוד IT ותוכנה. הרכיבים של ישות מרוכבת זו משמשים יחד בסביבה המבצעית או תומכת לצורכי ביצוע משימה נתונה או לצורכי השגת מטרה, תמיכה או דרישת משימה ספציפית.
צריך	משמעות הגדרה זו היא שההשלכות יובנו באופן מלא ויוערכו בקפידה.
תקרית אבטחה	אירועי אבטחה מוגדרים כאירועים הכוללים, אך אינם מוגבלים ל: • ניסיונות (נכשלו או הצליחו) לקבלת גישה בלתי מורשית למערכת או לנתונים שלה. • הפרעה בלתי רצויה או מניעת שירות. • שימוש לא מורשה במערכת לעיבוד או לאחסון של נתונים. • שינויים במאפייני החומרה, הקושחה או התוכנה במערכת ללא ידיעת הבעלים, הוראתו או הסכמתו. • נקודת חולשה באפליקציה שמובילה לגישה בלתי מורשית לנתונים.
מחשב וירטואלי:	הסביבה המלאה התומכת בהפעלה של תוכנות מתארחות. הערה – מחשב וירטואלי הוא מעטפת מלאה של החומרה הווירטואלית, הדיסקים הווירטואליים והמטה-נתונים המשויכים אליו. מחשבים וירטואליים מאפשרים ריבוי של מחשבים פיזיים בסיסיים המופעלים דרך שכבת תוכנה הנקראת Hypervisor.

סודיות בנקאית

פיקוח נוסף על סודיות בנקאית (שווייץ/מונקו)

גרסה סופית 14.0, אוקטובר 2024

אזור/תפקיד מפוקח	תיאור הפיקוח	מדוע זה חשוב
1. תפקידים ותחומי אחריות	על הספק להגדיר ולתקשר תפקידים, תחומי אחריות ויכולות חשבונאיות לטיפול בנתונים המזהים את הלקוח (להלן "CID:"). על הספק לעיין במסמכים המדגישים תפקידים, תחומי אחריות ויכולות חשבונאיות עבור CID לאחר כל שינוי מהותי במודל התפעולי של הספק (או הארגון) או לפחות פעם בשנה ולהפיץ אותם בתחום הסודיות הבנקאית המתאים. תפקידי מפתח חייבים לכלול מנהל בכיר, האחראי על פעילויות ההגנה והפיקוח על כל הפעילויות הקשורות ל-CID (יש לעיין בנספח א' להגדרות ה-CID). יש להקפיד שמספר אנשי ה-CID מינימלי, בהתאם לעקרון 'הצורך לדעת'.	הגדרה ברורה של תפקידים ותחומי אחריות תומכת ביישום לוח הזמנים של הפיקוח על ספקים חיצוניים.
2. דיווח על פריצת CID	יש לבצע בקרות, תהליכים ונהלים מתועדים כדי להבטיח שדיווחים וניהול על כל הפרה המשפיעה על CID. כל הפרה של דרישות הטיפול (כהגדרתן בטבלה B2) חייבת להינתן על ידי הספק ולדווח לישות הרלוונטית של Barclays בכפוף לסודיות בנקאית באופן מיידי (לא יאוחר מ-24 שעות). תהליך תגובה לאירוע לטיפול בזמן ודיווח קבוע על אירועים הקשורים ל-CID חייב להיקבע ולהיבדק באופן קבוע. על הספק לוודא ביצוע של פעולות מתקנות ולאחר מכן לוודא שהתקרית מטופלת במסגרת התוכנית המתקנת הרלוונטית (פעולה, בעלות, תאריך מסירה) ששותפה עם Barclays וקיבלה את הסכמתה, בהתאם לסודיות הבנקאית הרלוונטית בתחום השיפוט. על הספק ליישם פעולה מתקנת תוך פרק זמן סביר. במקרה שספק חיצוני המספק שירותי ייעוץ ובמקרה שעובד של ספק זה הפעיל תקריות למניעת אובדן נתונים, הבנק יודיעל התקרית לספק וכשהדבר רלוונטי, לבנק עומדת הזכות לבקש להחליף את העובד.	תהליך תגובה לאירועים עוזר להבטיח הכלה מהירה של האירועים ומניעת הסלמה. כל הפרה שתשפיע על CID עלולה לפגוע באופן ניכר במוניטין וב-Barclays ואף להוביל להשתת קנסות ולאובדן רישיון הבנקאות בשווייץ או במונקו
3. הדרכה ומודעות	עובדי ספקים עם גישה ל-CID חייבים להשלים הכשרה* המכסה את דרישות הסודיות הבנקאית בהקשר של CID לאחר כל שינוי בתקנות או לפחות פעם בשנה. הספק חייב להבטיח כי כל עובד החדש (עם גישה ל-CID) ישלים הכשרה המבטיחה שהוא מבין את תחומי האחריות שלו לגבי CID תוך פרק זמן סביר (עד 3 חודשים). הספק חייב לנטר עובדים שהשלימו את ההכשרה. * תחומי שיפוט בהקשר של סודיות בנקאית שמיועדים לספק הנחיות לגבי תוכן ההדרכה הנדרש.	פעילויות הדרכה והמודעות תומכות בכל אמצעי הפיקוח האחרים במסגרת לוח זמנים זה.

4. סכמת סימון מידע	***במקרה הצורך****, הספק חייב להחיל את סכמת סימון המידע של Barclays (טבלה E1 בנספח E) או תוכנית חלופית המוסכמת על סמכות השיפוט של סודיות בנקאית, בהקשר של כל נכסי המידע המוחזקים או המעובדים בשם הסודיות הבנקאית. דרישות הטיפול בנתוני CID מצוינות בטבלה E2 בנספח E. **'בהתאם לרלוונטיות'** *מתייחס לתועלת של תיוג מאוזן כנגד הסיכון הנלווה. למשל, יהיה זה בלתי הולם לתייג מסמך אם פעולה זו תפר את הדרישות הרגולטוריות למניעת חבלה.*	מלאי מלא ומדויק של נכסי המידע חיוני להבטחת יישום אמצעי פיקוח הולמים.
5. מחשוב ענן/אחסון חיצוני	כל השימוש במחשוב ענן ו/או באחסון חיצוני של CID (בשרתים מחוץ לתחום השיפוט של הסודיות הבנקאית או מחוץ לתשתית הספקים) המשמשים כחלק מהשירות לתחום השיפוט חייב להיות מאושר על-ידי צוותים מקומיים רלוונטיים מתאימים (כולל משרד האבטחה הראשי, צוות הציות והמחלקה המשפטית). בנוסף, יש ליישם אמצעי פיקוח בהתאם לחוקים ולתקנות החלים בתחום השיפוט המקביל של הסודיות הבנקאית כדי להגן על מידע CID בהתאם לפרופיל הסיכון הגבוה שהם מציגים.	אם עיקרון זה לא יושם, נתוני לקוח המוגנים באופן בלתי הולם (CID) עלולים להיפגע, מה שעלול לגרום להשתת סנקציות חוקיות ורגולטוריות ואף להוביל לפגיעה במוניטין.

נספח ב': מילון מונחים

** נתוני זיהוי הלקוח נחשבים נתונים מיוחדים בשל חוקי הסודיות הבנקאית החלים בשווייץ ובמונקו. ככאלה, אמצעי הפיקוח המפורטים להלן נועדו להשלים את אלה המפורטים לעיל.

תנאים	הגדרה
CID	נתונים מזהים של לקוח
CIS	אבטחת סייבר ומידע
עובד ספק	כל גורם המועסק על ידי הספק כעובד קבוע או כל גורם המספק שירותים לספק למשך פרק זמן מוגבל (כגון יועץ)
נכס	כל פיסת מידע או קיבוץ של פריטי מידע שיש להם ערך עבור הארגון
מערכת	מערכת, בהקשר של מסמך זה, היא אנשים, נהלים, ציוד IT ותוכנה. הרכיבים של ישות מרוכבת זו משמשים יחד בסביבה המבצעית או תומכת לצורכי ביצוע משימה נתונה או לצורכי השגת מטרה, תמיכה או דרישת משימה ספציפית.
מזהה משתמש	חשבון שהוקצה לעובד ספק, יועץ, קבלן או עובד של סוכנות כוח אדם שקיבל גישה למערכת בבעלות Barclays ללא הרשאות ברמה גבוהה יותר.

נספח ג': הגדרת נתונים מזהים של לקוחות

CID ישיר (DCID) יכול להיות מוגדר כמזהים ייחודיים (בבעלות הלקוח), המאפשרים, כפי שהם בפני עצמם, לזהות לקוח ללא צורך בגישה לנתונים כלשהם באפליקציות בנקאיות של Barclays. הוראה זו חייבת להיות חד משמעית, בלא כפיפות כלשהי לפרשנות ויכולה לכלול מידע כגון שם פרטי, שם משפחה, שם חברה, חתימה, מזהה רשת חברתית וכו'. CID ישיר מתייחס לנתוני לקוח שאינם בבעלות הבנק ולא נוצרו על ידו.

CID עקיף (ICID) – מחולק ל-3 רמות

- **L1 ICID**: ניתן להגדירו כמזהים ייחודיים (בבעלות הבנק) המאפשרים לזהות באופן ייחודי לקוח במקרים שבהם ניתנת גישה לאפליקציות בנקאיות או **לאפליקציות אחריות של צדדים שלישיים**. המזהה חייב להיות חד משמעי, לא כפוף לפרשנות, ועשוי לכלול מזהים כגון מספר חשבון, קוד IBAN, מספר כרטיס אשראי וכו'.
- **L2 ICID:** ניתן להגדירו כמידע (בבעלות הלקוח) אשר, בשילוב עם מידע אחר, יאפשר להסיק את זהותו של הלקוח. אמנם לא ניתן להשתמש במידע כגון זה כדי לזהות לקוח בפני עצמו, אך ניתן להשתמש בו בשילוב עם מידע אחר כדי לזהות לקוח. L2 ICID חייב להיות מוגן ומנוהל באותה רמת הקפדה כמו DCID.
- **L3 ICID:** ניתן להגדירו כמזהים ייחודיים אך אנונימיים (בבעלות הבנק), המאפשרים לזהות לקוח אם מוענקת גישה לאפליקציות בנקאיות. ההבדל עם L1 ICID הוא סיווג המידע כ'מוגבל – חיצוני' במקום הסיווג 'סודיות בנקאית', כלומר, הם אינם כפופים לאותו אמצעי פיקוח.

יש לעיין באיור 1: 'CID – עץ החלטות' כדי לקבל סקירה כללית של שיטת הסיווג.

אין לשתף נתוני L1 ICID, הן באופן ישיר והן בעקיפין, עם כל גורם שאינו נכלל במסגרת כוח האדם של הבנק ויש להקפיד על עקרון 'הצורך לדעת' בכל עת. ניתן לשתף נתוני L2 ICID על בסיס עקרון 'הצורך לדעת', אך אין לשתפם בשילוב עם כל פיסת CID אחרת. שיתוף נתוני CID שונים מאפשרים ליצור 'שילוב נתונים רעיל' כדי לחשוף את זהותו של הלקוח. שילוב רעיל נקבע עבור חשיפת שני רכיבי L2 ICID לפחות. ניתן לשתף נתוני L3 ICID מכיוון שהם אינם מסווגים כמידע ברמת 'סודיות בנקאית', אלא אם שימוש חוזר באותו מזהה יכול לגרום לאיסוף מספיק של נתוני L2 ICID כדי לחשוף את זהותו של הלקוח.

סיווג מידע	סודיות בנקאית			מוגבל – פנימי
סיווג	**CID ישיר (DCID)**	**CID עקיף (ICID)**		
		עקיף (L1)	**עקיף מבחינה פוטנציאלית (L2)**	**מזהה שאינו אישי (L3)**
סוג המידע	שם לקוח/לקוח פוטנציאלי	מספר מכל/מזהה מכל	מקום לידה	כל מזהה פנימי של אירוח CID/אפליקציית עיבוד
	שם חברה	MACC (חשבון מוניטרי תחת מזהה מכל Avaloq)	תאריך לידה	מזהה דינמי
	דף חשבון	מזהה SDS	אזרחות	מזהה CRM Party Role
	חתימה	IBAN	תואר	מזהה גורם מכיל חיצוני
	מזהה ברשת חברתית	פרטי כניסה אל eBanking	מצב משפחתי	
	מספר דרכון	מספר כספת	מיקוד	
	מספר טלפון	מספר כרטיס אשראי	הון עצמי	
	כתובת דוא"ל	הודעת SWIFT	מיקום Large/ערך עסקה	
	שם תפקיד או כותרת PEP	מזהה פנימי של שותף עסקי	ביקור אחרון של הלקוח	
	שם האמן		שפה	
	כתובת IP		מין	
	מספר פקס		תאריך תפוגת CC	
			איש קשר ראשי	
			מקום לידה	
			תאריך פתיחת חשבון	

דוגמה: במקרה של שליחת הודעת דוא"ל או שיתוף מסמך כלשהו עם גורמים חיצוניים (לרבות צדדים שלישיים בשווייץ/מונקו) או עם עמיתים בארגון/בחברה בת אחרת הפועלת בשווייץ/מונקו או במדינות אחרות (כגון בריטניה)

1. שם לקוח

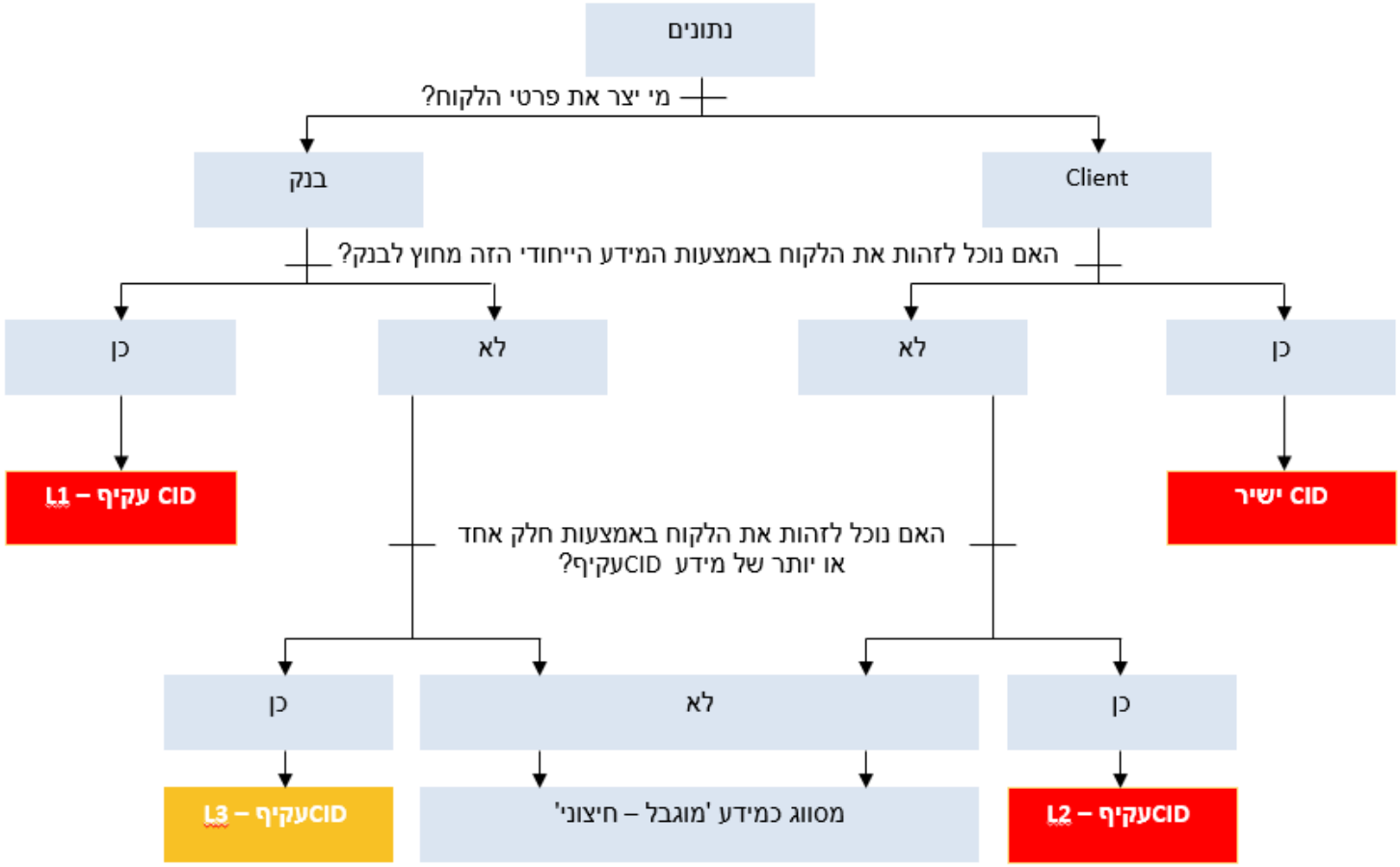
   (DCID) = הפרת סודיות בנקאית

2. מזהה מכל

   (L1 ICID) = הפרת סודיות בנקאית

3. הון עצמי + אזרחות

הפרת סודיות בנקאית = (L2 ICID) + (L2 ICID)



נספח ד': סכימת הסימון והמידע של Barclays

טבלה D1: סכימת הסימון והמידע של Barclays

** תווית הסודיות הבנקאית היא ספציפית לתחום השיפוט החל על הסודיות הבנקאית.

תווית	הגדרה	דוגמאות
סודיות בנקאית	כל מידע הקשור לנתוני זיהוי לקוח (CID), במישרין או בעקיפין, של לקוח בשווייץ. הסיווג 'סודיות בנקאית' חל על מידע הקשור לכל נתוני זיהוי לקוח, הן במישרין והן בעקיפין. לכן, מתן גישה לכל עובדי הארגון, אפילו לכאלה הפועלים בתחום השיפוט החל על בעלי המידע אינו הולם. גישה למידע זה נדרשת רק על ידי אלה עם 'הצורך לדעת' כדי שיוכלו למלא את חובותיהם הרשמיות או לקיים את האחריות החוזית שלהם. חשיפה, גישה או שיתוף בלתי מורשים, הן באופן פנים ארגוני והן באופן חיצוני, של מידע כגון זה עלולה להשית השפעה קריטית ואף להוביל להליכים פליליים, עם השלכות אזרחיות ומנהליות, כגון הטלת קנסות ואובדן הרישיון הבנקאי, במקרה של חשיפת המידע לגורמים בלתי מורשים, הן באופן פנים ארגוני והן באופן חיצוני.	• שם לקוח • כתובת לקוח • חתימה • כתובת ה-IP של הלקוח (דוגמאות נוספות בנספח D)

תווית	הגדרה	דוגמאות
סוד	מידע חייב להיות מסווג כ'סוד', אם לחשיפה הבלתי מורשית שלו תהיה השפעה שלילית על Barclays, אם הערכה המתבצעת במסגרת Enterprise Risk Management Framework (ERMF) קבעה כי חשיפה כגון זאת היא "קריטית' (פיננסית או כזו שאינה פיננסית). מידע זה מוגבל לקהל יעד מסוים ואין להפיצו הלאה ללא אישור היוצר. הקהל היעד עשוי לכלול נמענים חיצוניים, לאחר קבלת אישור מפורש מבעלי המידע.	• מידע על מיזוגים או רכישות פוטנציאליות. • תכנון אסטרטגי – מידע עסקי וארגוני. • מידע מסוים אודות תצורת אבטחת מידע. • דוחות וממצאי ביקורת מסוימים. • סיכום דיוני מועצת המנהלים. • אימות או זיהוי ואישור (ID&V) פרטים – לקוח/לקוח ועמית. • כמויות מידע גדולות של מחזיק הכרטיס. • תחזיות רווח או דוחות פיננסיים שנתיים (לפני פרסומם לציבור). • כל הפריטים המכוסים במסגרת הסכם סודיות (NDA) רשמי.

מוגבל – פנימי	יש לסווג את המידע כ'מוגבל – פנימי', אם הנמענים הצפויים הם עובדים מאומתים של Barclays וספקי שירות מנוהלים של Barclays (MSP) בלבד הפועלים במסגרת חוזה פעיל וכשהמידע מוגבל לקהל יעד מסוים. לחשיפה בלתי מורשית תהיה השפעה שלילית על Barclays, שהערכתה במסגרת ERMF היא 'מהותית' או 'מוגבלת' (הן מבחינה פיננסית והן מבחינה שאינה פיננסית). מידע כגון זה אינו מיועד להפצה כללית, אך ייתכן שיועבר לנמענים או ישותף על ידם בהתאם לעקרון הצורך לדעת.	• אסטרטגיות ותקציבים. • הערכות ביצועים. • שכר עובדים ומידע אישי. • הערכת נקודות תורפה . • דוחות וממצאי ביקורת.
מוגבל – חיצוני	יש לסווג את המידע כמוגבל – חיצוני, אם הנמענים הצפויים הם עובדים מאומתים של Barclays ו-ספקי שירות מנוהלים של Barclays (MSP) בלבד הפועלים במסגרת חוזה פעיל וכשהמידע מוגבל לקהל מסוים או לצדדים חיצוניים שקיבלו הרשאה של בעלי המידע. לחשיפה בלתי מורשית תהיה השפעה שלילית על Barclays, שהערכתה במסגרת ERMF היא 'מהותית' או 'מוגבלת' (הן מבחינה פיננסית והן מבחינה שאינה פיננסית). מידע כגון זה אינו מיועד להפצה כללית, אך ייתכן שיועבר לנמענים או ישותף על ידם בהתאם לעקרון הצורך לדעת.	• תוכניות מוצר חדשות. • חוזים עם לקוחות. • חוזים משפטיים. • לקוחות בודדים/לקוחות בהיקף עסקי נמוך/פרטי לקוחות למשלוח לגורמים חיצוניים. • לקוחות/תקשורת עם לקוחות. • הצעות חדשות (למשל, תשקיף, מזכר הצעה). • מסמכי מחקר סופיים. • מידע שאינו בבעלות Barclays ואינו מהווה מידע ציבורי (MNPI). • דוחות מחקר מכול סוג • חומרי שיווק מסוימים. • פרשנות השוק.
בלתי מוגבל	יש לסווג את המידע כבלתי מוגבל, אם הפצתו היא כללית או אם לחשיפתו לא תהיה השפעה שלילית על הארגון.	• חומרי שיווק. • פרסומים. • הודעות לציבור. • פרסומות בנושא העסקה. • מידע שאין לו כל השפעה על Barclays.

טבלה D2: סכמת תיוג מידע – דרישות לטיפול בנתונים

** דרישות טיפול ספציפיות לנתוני CID, על מנת להבטיח את סודיות המידע, בהתאם לדרישות הרגולטוריות

שלב מחזור חיים	דרישות סודיות בנקאית
יצירה וסימון	בהתאם להוראה 'מוגבל–חיצוני' וכן: • יש להקצות נכסים לבעלי CID.
אחסון	בהתאם להוראה 'מוגבל–חיצוני' וכן: • יש לאחסן את הנכסים במדיה נשלפת כל עוד הדבר נדרש במפורש עבור צורך עסקי ספציפי, בהתאם להוראה רגולטורית או בהתאם לבקשה של רואי חשבון חיצוניים. • אין לאחסן כמויות גדולות של נכסי מידע העוסקים בסודיות בנקאית בהתקני מדיה/בהתקנים ניידים. לקבלת מידע נוסף, יש לפנות לצוות המקומי לאבטחת סייבר ומידע (להלן CIS). • אין לאחסן נכסים (בין אם פיזיים ובין אם אלקטרוניים) בסביבה שבה גורמים בלתי מורשים עשויים לקבל גישה או להציג נתונים כגון אלה, בהתאם לעיקרון 'הצורך לדעת'. • יש להקפיד על נהלי עבודה מאובטחים, כגון Clear Desk ו-Desktop Locking, כדי להבטיח אבטחה הולמת של הנכסים (פיזיים או אלקטרוניים). • יש להשתמש בנכסי מידע המאוחסנים בהתקני מדיה נשלפים כל הדבר נדרש במפורש ולנעול אותם כשאינם בשימוש. • העברת נתונים אד-הוק להתקני מדיה/אחסון ניידים מחייבת אישור של בעלי הנתונים, להתבצע בהתאם לתאימות ולאחר קבלת אישור CIS.
גישה ושימוש	בהתאם להוראה 'מוגבל–חיצוני' וכן: • אין להסיר או להציג נכסים מחוץ לאתר (מתחמים של Barclays) ללא אישור רשמי של בעלי ה-CID (או סגנו). • אין להסיר או להציג נכסים מחוץ לתחום השיפוט החל על הזמנת הלקוח ללא אישור רשמי מבעלי ה-CID (או סגנו) והלקוח (כתב ויתור/ייפוי כוח מוגבל). • יש לפעול בהתאם להנחיות לעבודה מאובטחת מרחוק, המבטיחים כי אין אפשרות לזליגת מידע בשל 'עיניים טועות' בעת הוצאת נכסים מחוץ לאתר.
	• יש לוודא שגורמים בלתי מורשים לא יוכלו לצפות או לגשת לנכסים האלקטרוניים המכילים CID באמצעות שימוש ביכולת גישה מוגבלת לאפליקציות עסקיות.
שיתוף	בהתאם להוראה 'מוגבל–חיצוני' וכן: • יש להפיץ נכסים רק בהתאם לעיקרון 'הצורך לדעת' ובמסגרת מערכת הסודיות הבנקאית המקורית של מערכת המידע וצוות העובדים. • נכסים המופצים על בסיס אד-הוק באמצעות מדיה נשלפת מחייבים אישור של בעלי נכסי המידע ואישור CIS. • תקשורת אלקטרונית חייבת להיות מוצפנת במהלך מעבר. • נכסים (עותק קשיח) הנשלחים בדואר חייבים להימסר באמצעות שירות המחייב קבלת אישור.

	• יש להפיץ את הנכסים רק בהתאם לעקרון 'הצורך לדעת'.
אחסון בארכיון והשלכה	בהתאם להוראה 'מוגבל–חיצוני'

*** מידע אודות תצורת אבטחת המערכת, ממצאי ביקורת ורשומות אישיות עשויים להיות לקבל את הסיווג 'מוגבל–פנימי' או את הסיווג 'סוד', בהתאם להשפעה של חשיפה בלתי מורשית על הפעילות העסקית

שלב מחזור חיים	מוגבל – פנימי	מוגבל – חיצוני	סוד
יצירה והצגה	• יש להקצות נכסים לבעלי נכסי המידע.	• יש להקצות נכסים לבעלי נכסי המידע.	• יש להקצות נכסים לבעלי נכסי המידע.
אחסון	• אין לאחסן נכסים (בין אם פיזיים ובין אם אלקטרוניים) באזורים ציבוריים (לרבות אזורים ציבוריים במתחמים שבהם תיתכן גישה של מבקרים ללא פיקוח הולם). • אין להשאיר מידע באזורים ציבוריים במתחמים שבם תיתכן גישה של מבקרים ללא פיקוח הולם.	• אין לאחסן נכסים (בין אם פיזיים ובין אם אלקטרוניים) במקום שבו גורמים בלתי מורשים עשויים לקבל גישה או להציג נתונים כגון אלה. • יש להגן על נכסים אלקטרוניים מאוחסנים באמצעות יישום הצפנה או אמצעי שיפוי הולמים אם קיים סיכון מהותי שגורמים בלתי מורשים יוכלו לקבל גישה לנתונים.	• אין לאחסן נכסים (בין אם פיזיים ובין אם אלקטרוניים) במקום שבו גורמים בלתי מורשים עשויים לקבל גישה או להציג נתונים כגון אלה. • יש להגן על נכסים אלקטרוניים מאוחסנים באמצעות יישום הצפנה או אמצעי שיפוי הולמים אם קיים סיכון מהותי שגורמים בלתי מורשים יוכלו לקבל גישה לנתונים. • על כל המפתחות הפרטיים המשמשים להגנה על נתונים, על זהות ו/או על המוניטין של Barclays להיות מוגנים באמצעות יישום מודולי אבטחת חומרה מאושרים (HSM) מסוג FIPS 140-2 Level 3.
גישה ושימוש	• אין להשאיר נכסים (פיזיים או אלקטרוניים) באזורים ציבוריים מחוץ למתחם. • אין להשאיר נכסים (פיזיים או אלקטרוניים) באזורים ציבוריים, במקומות שבהם מבקרים יוכלו לקבל גישה לנכסים ללא כל פיקוח.	• אין לעבוד על נכסים (פיזיים או אלקטרוניים) או להשאיר אותם ללא השגחה במקום שבו גורמים בלתי מורשים יוכלו להציג אותם או לקבל גישה אליהם. יש לעבוד על נכסים רק לאחר יישום אמצעי פיקוח נאותים (כגון מסכי פרטיות).	• אין לעבוד על נכסים (פיזיים או אלקטרוניים) או להשאיר אותם ללא השגחה במקום שבו גורמים בלתי מורשים יוכלו להציג אותם או לקבל גישה אליהם. יש לעבוד על נכסים רק לאחר יישום אמצעי פיקוח נאותים (כגון מסכי פרטיות).

	• יש להגן על נכסים אלקטרוניים באמצעות יישום אמצעי ניהול גישה לוגיים הולמים, במידת הצורך	• לאחר הדפסת נכס כלשהו, יש לקחת את פלט ההדפסה באופן מיידי מהמדפסת. אם הדבר אינו אפשרי, יש להשתמש במדפסת מאובטחת. • יש להגן על נכסים אלקטרוניים באמצעות יישום אמצעי ניהול גישה לוגיים הולמים.	• יש להדפיס נכסים רק באמצעות מדפסות מאובטחות. • יש להגן על נכסים אלקטרוניים באמצעות יישום אמצעי ניהול גישה לוגיים הולמים
שיתוף	• יש להצמיד לעותק קשיח תווית מידע גלויה. יש להצמיד את התווית לעמוד הכותרת לכל הפחות. • נכסים אלקטרוניים חייבים לשאת תווית מידע ברורה. • יש להפיץ נכסים רק באמצעות מערכות, שיטות או ספקים שאושרו על ידי הארגון. • נכסים חייבים להיות מופצים רק לגורמים המועסקים על ידי הארגון או כאלה שפועלים במסגרת חוזית מתאימה או כחלק מצרך עסקי מוכר בבירור, כגון משא ומתן חוזי.	• יש להצמיד לעותקי חוזים תווית מידע גלויה. יש להצמיד את התווית לעמוד הכותרת לכל הפחות. • מעטפות המכילות עותקי נכסים קשיחים חייבות לשאת תווית מידע גלוי בחזיתן • נכסים אלקטרוניים חייבים לשאת תווית מידע ברורה. עותקים אלקטרוניים של מסמכים מרובי עמודים חייבים לשאת תווית מידע גלויה שתוצמד על כל אחד מהעמודים. • יש להפיץ נכסים רק באמצעות מערכות, שיטות או ספקים שאושרו על ידי הארגון. • נכסים חייבים להיות מופצים רק לגורמים המועסקים על ידי הארגון או כאלה שפועלים במסגרת חוזית מתאימה או כחלק מצרך עסקי מוכר בבירור, כגון משא ומתן חוזי. • נכסים חייבים להיות מחולקים רק לגורמים שלהם צורך עסקי לקבלם. • אין לשלוח עותקי נכסים בפקס, אלא אם השולח אישר שהנמענים מוכנים ויכולים לקבל את עותקי הנכסים באופן מיידי. • יש להצפין נכסים אלקטרוניים באמצעות שימוש במנגנון הגנה קריפטוגרפי מאושר כשהם במעבר מחוץ לרשת הפנים ארגונית.	• עותקים קשיחים של נכסים חייבים לשאת תווית מידע גלויה שמוצמדת לכל אחד מהעמודים. • מעטפות המכילות עותקים קשיחים של נכסים חייבות לשאת תווית מידע גלוי בחזיתן ולהיות חתומות באמצעות חותם ברור. לפני הפצתם, יש להניחם בתוך מעטפה משנית שאינה כוללת תווית כלשהי. • נכסים אלקטרוניים חייבים לשאת תווית מידע ברורה. עותקים אלקטרוניים של מסמכים מרובי עמודים חייבים לשאת תווית מידע גלויה שתוצמד על כל אחד מהעמודים. • יש להפיץ נכסים רק באמצעות מערכות, שיטות או ספקים שאושרו על ידי הארגון. • נכסים חייבים להיות מופצים רק לגורמים המועסקים על ידי הארגון או כאלה שפועלים במסגרת חוזית מתאימה או כחלק מצרך עסקי מוכר בבירור, כגון משא ומתן חוזי. • יש להפיץ נכסים רק לגורמים שקיבלו אישור לקבלם מהבעלים של נכסי המידע. • אין לשלוח נכסים בפקס. • יש להצפין נכסים אלקטרוניים באמצעות שימוש במנגנון הגנה קריפטוגרפי מאושר כשהם במעבר מחוץ לרשת הפנים ארגונית.

			• יש להקפיד על שרשרת המשמורת על נכסים אלקטרוניים.
אחסון בארכיון והשלכה	• יש להשליך עותקים קשיחים של נכסים באמצעות שירות פסולת חסוי. • עותקים של נכסים אלקטרוניים חייבים להימחק גם מ'פחי המיחזור' של המערכת או התקנים דומים במועד	• יש להשליך עותקים קשיחים של נכסים באמצעות שירות פסולת חסוי. • עותקים של נכסים אלקטרוניים חייבים להימחק גם מ'פחי המיחזור' של המערכת או התקנים דומים במועד.	• יש להשליך עותקים קשיחים של נכסים באמצעות שירות פסולת חסוי. • עותקים של נכסים אלקטרוניים חייבים להימחק גם מ'פחי המיחזור' של המערכת או התקנים דומים במועד. • התקן מדיה שבה אוחסנו נכסים אלקטרוניים סודיים חייב לעבור תהליך סניטציה הולם לפני או במהלך השלכה.