مستند متطلبات نظام الحضور الذكي المتكامل

الإصدار: 1.0 (مسودة أولى)
تاريخ: [25-10-2025]
المؤلف: **م. فراس عزالدين سويد**.

---

1. المقدمة (Introduction)

1.1. الغرض (Purpose)

الغرض من هذا المستند (SRS - Software Requirements Specification) هو تقديم وصف تفصيلي وشامل لنظام الحضور الذكي المقترح. يعمل هذا المستند كمرجع أساسي ودليل موحد لجميع أصحاب المصلحة (Stakeholders)، بما في ذلك فريق التطوير، مديري المشاريع، وفريق ضمان الجودة. يهدف إلى تحديد وتوثيق جميع المتطلبات الوظيفية (Functional Requirements) وغير الوظيفية (Non-Functional Requirements) للنظام، بالإضافة إلى القيود والمعايير التي يجب أن يلتزم بها.

سيضمن هذا المستند أن هناك فهمًا مشتركًا وواضحًا للمنتج النهائي، مما يقلل من احتمالية سوء الفهم ويسهل عملية التصميم، التطوير، الاختبار، والنشر.

1.2. نطاق النظام (System Scope)

النظام المقترح، الذي سيُشار إليه باسم "نظام الحضور الذكي"، هو حل برمجي متكامل يهدف إلى أتمتة وتبسيط عملية تسجيل وإدارة حضور وانصراف الموظفين، مصمم خصيصًا لتلبية احتياجات الشركات التي تمتلك عددًا كبيرًا من الموظفين الموزعين عبر مواقع جغرافية متعددة أو الذين يعملون في الميدان.

سيقوم النظام باستبدال أو تعزيز أنظمة الحضور التقليدية (مثل أجهزة البصمة المادية أو السجلات اليدوية) من خلال توفير منصة مركزية وآمنة تعتمد على الهواتف الذكية.

المكونات الرئيسية للنظام تشمل:

1. **تطبيق للهواتف الذكية (Android & iOS):** سيستخدمه الموظفون لتسجيل الحضور والانصراف باستخدام آليات تحقق متقدمة مثل التحقق من الموقع الجغرافي (Geofencing) والتعرف الآلي على الوجه (Face Recognition).
2. **لوحة تحكم قائمة على الويب (Web-based Dashboard):** ستستخدمها الإدارة (بمختلف مستوياتها) لمراقبة بيانات الحضور في الوقت الفعلي، إدارة بيانات الموظفين والهيكل التنظيمي، إنشاء وتصدير التقارير، وإدارة السياسات والقواعد الخاصة بالنظام.

الوظائف الرئيسية التي سيغطيها النظام (In-Scope):

- إدارة ملفات الموظفين والهيكل التنظيمي (فروع، فرق).
- تسجيل الحضور والانصراف بآليات متعددة وآمنة.
- إدارة الجداول الزمنية والورديات وسياسات الحضور المرنة.
- تتبع الحالات المختلفة للحضور (حاضر، متأخر، غائب، إجازة، إلخ).
- آلية للتحقق الدوري من تواجد الموظفين خلال ساعات العمل.
- نظام إشعارات تفاعلي لجميع فئات المستخدمين.
- إنشاء تقارير تحليلية ومفصلة عن الحضور.

ما هو خارج نطاق النظام (Out-of-Scope) في هذه المرحلة:

- إدارة الرواتب (Payroll System). (النظام سيُصدّر بيانات يمكن استخدامها في أنظمة الرواتب، ولكنه لن يقوم بحساب الرواتب بنفسه).
- نظام إدارة الموارد البشرية الكامل (HRMS)، مثل تقييم الأداء أو تتبع التوظيف.
- إدارة المخزون أو الأصول.

1.3. التعريفات، المختصرات، والمصطلحات (Definitions, Acronyms, and Abbreviations)

يسرد هذا القسم تعريفات جميع المصطلحات والمختصرات المستخدمة في المستند لضمان فهم موحد ودقيق من قبل جميع القراء.

المصطلح / المختصر	التعريف الكامل	الوصف
SRS	Software Requirements Specification	"مستند متطلبات النظام"، وهو المستند الذي نقوم بكتابته الآن.
النظام	نظام الحضور الذكي	الإشارة إلى المشروع بأكمله، بما في ذلك تطبيق الهاتف ولوحة التحكم.

تطبيق الموظف	Mobile Application	التطبيق الذي يتم تثبيته على هواتف الموظفين (Android/iOS).
لوحة التحكم	Dashboard / Admin Panel	الواجهة المستندة إلى الويب والمخصصة للمستخدمين الإداريين (المشرفون، مديرو الموارد البشرية، ومسؤولو النظام).
بصمة الوجه (Faceprint)	Face Embedding / Vector	التمثيل الرياضي الرقمي لملامح وجه الموظف (متجه من 128 بُعدًا)، ويستخدم للمقارنة والتحقق بدلاً من تخزين الصور.
ML Kit	Google Machine Learning Kit	مجموعة أدوات من جوجل لتنفيذ وظائف تعلم الآلة على الهواتف، مثل اكتشاف الوجوه.
TFLite	TensorFlow Lite	نسخة خفيفة من إطار عمل TensorFlow مصممة لتشغيل نماذج تعلم الآلة على الأجهزة المحمولة والمدمجة.
السياج الجغرافي (Geofence)	Geographical Fence	حدود جغرافية افتراضية (عادةً دائرة) تُعرّف منطقة العمل المسموح بها للموظف.

الموقع الوهمي	Mock Location / Fake GPS	ميزة في نظام التشغيل (عادةً في خيارات المطور) تسمح للمستخدم بتزييف موقعه الجغرافي عبر تطبيقات خارجية.
سجل التدقيق	Audit Log / Audit Trail	سجل زمني متسلسل وغير قابل للتغيير لجميع الإجراءات والعمليات الهامة التي تحدث في النظام.
HR	Human Resources	قسم الموارد البشرية في الشركة.
API	Application Programming Interface	واجهة برمجة التطبيقات التي تسمح لتطبيق الهاتف بالتواصل مع السيرفر.
SDK	Software Development Kit	حزمة أدوات التطوير البرمجي.
UI	User Interface	واجهة المستخدم.

1.4. المراجع (References)

يسرد هذا القسم أي مستندات أو مصادر خارجية تم الاستناد إليها أثناء إعداد هذا المستند.

- **[مرجع 1]** وثيقة Google FaceNet البحثية: *"FaceNet: A Unified Embedding for Face Recognition and Clustering"* - Schroff, F., Kalenichenko, D., & Philbin, J. (2015). (كمرجع أساسي للمنهجية التقنية للتعرف على الوجه).
- **[مرجع 2]** وثائق Google ML Kit الرسمية. (للتفاصيل الفنية حول اكتشاف الوجوه).
- **[مرجع 3]** وثائق TensorFlow Lite الرسمية. (للتفاصيل الفنية حول تشغيل النماذج على الأجهزة).

1.5. نظرة عامة على المستند (Document Overview)

يقدم هذا المستند وصفًا شاملاً لنظام الحضور الذكي. وهو منظم على النحو التالي:

- **القسم 1 - المقدمة:** يقدم هذا القسم، ويحدد الغرض من المستند ونطاق النظام والتعريفات والمصطلحات الأساسية.
- **القسم 2 - الوصف العام:** يوفر نظرة عامة على النظام من منظور أعلى، ويصف وظائفه الرئيسية، وخصائص المستخدمين، والقيود والافتراضات العامة التي تحكم المشروع.
- **القسم 3 - المتطلبات المحددة:** هذا هو الجزء الأكثر تفصيلاً في المستند. يحدد جميع المتطلبات الوظيفية وغير الوظيفية، ومتطلبات الواجهات الخارجية التي يجب على النظام تحقيقها.

---

2. الوصف العام (Overall Description)

منظور المنتج (Product Perspective)

نظام الحضور الذكي هو نظام معلوماتي مستقل بذاته ومكتفٍ ذاتيًا (self-contained). لا يعتمد النظام على أنظمة برمجية أخرى ليعمل، ولكنه مصمم ليكون قابلاً للتكامل مع أنظمة الموارد البشرية (HRMS) وأنظمة الرواتب (Payroll Systems) الأخرى في المستقبل عن طريق تصدير البيانات بصيغ قياسية (مثل CSV أو Excel) أو من خلال توفير واجهة برمجة تطبيقات (API) مخصصة لهذا الغرض.

الغرض الأساسي من المنتج هو توفير حل مركزي وحديث ليحل محل الأساليب التقليدية لتتبع الحضور والتي ثبت عدم فعاليتها في بيئات العمل الحديثة التي تتميز باللامركزية الجغرافية والتنوع في طبيعة وظائف الموظفين (مكتبي، ميداني، عن بعد). النظام لا يقوم بتعديل أو استبدال أي نظام حاسم حالي في الشركة، بل يضيف قدرة جديدة وأساسية للإدارة الفعالة للقوى العاملة.

2.1. دراسة الجدوى والقيمة المقترحة (Business Case and Value Proposition)

2.1.1. حل مشكلة عمل حرجة (Addressing a Critical Business Problem)

تواجه الشركات الحديثة، خاصة تلك التي تمتلك قوى عاملة كبيرة وموزعة جغرافيًا، تحديًا كبيرًا في إدارة وتتبع حضور الموظفين بفعالية. الأساليب التقليدية مثل أجهزة البصمة المادية أو السجلات الورقية أصبحت غير عملية وغير قادرة على مواكبة بيئات العمل الديناميكية. هذا القصور يؤدي مباشرة إلى:

- **بيانات غير دقيقة:** صعوبة جمع البيانات بشكل فوري وموحد من مواقع متعددة.
- **زيادة احتمالات التحايل:** مثل "التحضير بالنيابة" (Buddy Punching) أو تسجيل الحضور دون التواجد الفعلي في موقع العمل.

- **عبء إداري هائل:** استهلاك وقت وجهد كبيرين من قبل أقسام الموارد البشرية في جمع السجلات يدويًا، مراجعتها، وتجهيزها لكشوف الرواتب.
- **ضعف الرؤية الاستراتيجية:** عدم قدرة الإدارة العليا على الحصول على نظرة شاملة وفورية عن التزام القوى العاملة.

يأتي "نظام الحضور الذكي" ليقدم حلاً شاملاً ومباشرًا لهذه المشاكل من خلال أتمتة العملية بالكامل، مما يضمن الدقة، يعزز الشفافية، ويحرر الموارد الإدارية لمهام أكثر استراتيجية.

2.1.2. فلسفتنا الأساسية: الأمان، المرونة، والكفاءة (Core Philosophy: Security, Flexibility, and Efficiency)

تم تصميم وتطوير النظام بناءً على ثلاثة مبادئ أساسية مترابطة تضمن تقديم قيمة حقيقية ومستدامة:

- **الأمان أولاً (Security-First):**
نحن ندرك أن بيانات الحضور هي بيانات حساسة ومهمة. لذا، تم بناء النظام على أساس بنية أمنية متعددة الطبقات تهدف إلى ضمان الموثوقية ومنع التحايل. الآليات الرئيسية تشمل:
  1. **التحضير الذاتي الموثّق:** آلية تحقق متقدمة تتطلب تطابق هوية الجهاز، والموقع الجغرافي الدقيق، وبصمة الوجه الحية (مع التحقق من الحيوية)، مما يجعل أساليب التحايل الشائعة شبه مستحيلة.
  2. **التحضير عبر المشرف:** آلية بديلة موثوقة للحالات الاستثنائية، حيث تضع المسؤولية في يد قائد الفريق وتوثق العملية بالصورة والموقع، مما يضمن المساءلة والشفافية.
  3. **الإدخال اليدوي المُدقَّق:** آلية للطوارئ القصوى مخصصة للإدارة العليا فقط، مع فرض تسجيل إلزامي للسبب وتوثيق كامل في سجلات غير قابلة للتغيير، مما يمنع أي تلاعب غير مبرر.
- **المرونة القصوى (Maximum Flexibility):**
النظام مصمم ليتكيف مع الهيكل التنظيمي للشركة وليس العكس. بدلاً من فرض قواعد جامدة، يوفر النظام مرونة كاملة في تعريف الجداول الزمنية، سياسات الورديات، وفترات السماح، مع القدرة على تعيين هذه السياسات على مستوى الموظف الفردي، مما يسمح بالتعامل مع كافة الحالات الخاصة والاستثناءات بسهولة.
- **الكفاءة التشغيلية (Operational Efficiency):**
الهدف النهائي للنظام هو تبسيط العمليات وتوفير الوقت. يتم تحقيق ذلك من خلال أتمتة كاملة لعملية جمع البيانات، وتوفير إشعارات استباقية للموظفين والمدراء، وإنشاء تقارير آلية ودقيقة بضغطة زر. هذا يحرر وقت الموظفين الإداريين للتركيز على مهام ذات قيمة أعلى مثل تحليل البيانات وتطوير الموظفين بدلاً من إضاعته في أعمال المتابعة الروتينية.

2.1.3. الميزة التنافسية: بنية مستقلة بتكلفة تشغيلية منخفضة (Competitive Edge: Autonomous Architecture with Low Operational Cost)

على عكس العديد من الأنظمة الحديثة التي تعتمد بشكل كلي على المعالجة السحابية المستمرة والمكلفة، تم تصميم هذا النظام بفلسفة معمارية مبتكرة تسمى **"الذكاء على الحافة" (Intelligence at the Edge)**.

ماذا يعني هذا عمليًا؟

- **المعالجة على جهاز المستخدم:** يتم تفويض العمليات الحاسوبية المعقدة والمكلفة، مثل تحليل صورة الوجه وإنشاء بصمة الوجه، والتحقق الدوري من الموقع الجغرافي، ليتم تنفيذها مباشرة على معالج هاتف الموظف نفسه.

- **التأثير المباشر على البنية التحتية:** هذه البنية الذكية تقلل بشكل هائل من الحمل المستمر على خوادم النظام. فبدلاً من أن تقوم الخوادم بمعالجة عشرات الآلاف من الصور وطلبات الموقع في كل ساعة، يقتصر دورها على استلام نتائج جاهزة، وتنسيق العمليات، وتخزين البيانات النهائية.

النتيجة الاقتصادية والتقنية:
هذا التصميم لا يعزز سرعة الاستجابة للمستخدم النهائي فحسب، بل يؤدي مباشرةً إلى **فواتير استضافة شهرية منخفضة جدًا** مقارنة بالحلول المنافسة المعتمدة كليًا على السحابة. النظام مصمم ليكون مستدامًا اقتصاديًا وقابلاً للتوسع لخدمة آلاف المستخدمين دون أن يصاحب هذا النمو زيادة هائلة ومكلفة في الموارد السحابية المطلوبة. هذه الكفاءة في التكلفة تمثل ميزة تنافسية أساسية وقيمة طويلة الأمد للشركة.

2.1.4. ملخص المزايا: لماذا هذا النظام هو الخيار الأفضل؟ (Summary of Benefits: Why This System is the Optimal Choice?)

بناءً على ما سبق، يقدم نظام الحضور الذكي قيمة فريدة ومقنعة تجعله الخيار الأمثل لإدارة حضور الموظفين. يمكن تلخيص الفوائد الرئيسية في النقاط التالية:

- **أمان فائق وموثوقية عالية:**
بفضل آليات التحقق متعددة الطبقات (جهاز، موقع، وجه حي) وسجل التدقيق غير القابل للتغيير، يوفر النظام أعلى درجات الثقة في دقة بيانات الحضور ويقضي فعليًا على إمكانيات التحايل.
- **كفاءة إدارية منقطعة النظير:**
يوفر النظام الوقت والجهد بشكل كبير من خلال أتمتة عملية جمع البيانات، وتوفير تقارير آلية ودقيقة، وتمكين الإدارة من اتخاذ قرارات سريعة ومبنية على معلومات محدثة.
- **مرونة تتكيف مع احتياجات العمل:**
النظام ليس حلاً جامدًا؛ فهو مصمم للتكيف مع أعقد الهياكل التنظيمية والسياسات المختلفة للورديات والإجازات، مما يضمن ملاءمته لاحتياجات الشركة الحالية والمستقبلية.
- **تكلفة ملكية منخفضة ومستدامة:**
إن التصميم المعماري المبتكر الذي يعتمد على المعالجة اللامركزية يضمن أن تكاليف التشغيل الشهرية للبنية التحتية ستكون في حدها الأدنى، مما يوفر قيمة اقتصادية استثنائية على المدى الطويل.

2.2. وظائف المنتج الرئيسية (Major Product Functions)

يقدم النظام مجموعة متكاملة من الوظائف التي تخدم أصحاب المصلحة المختلفين. يمكن تلخيص الوظائف الرئيسية في النقاط التالية (سيتم تفصيل كل وظيفة لاحقًا في القسم 3):

- **إدارة المستخدمين والأدوار:**
  - إنشاء وإدارة حسابات لجميع مستخدمي النظام (موظفين، مشرفين، مدراء، ومسؤولين).
  - تحديد دقيق للصلاحيات بناءً على دور كل مستخدم.
- **إدارة الهيكل التنظيمي:**
  - تعريف وإدارة الفروع والمواقع الجغرافية المختلفة للشركة.

- تعريف وإدارة الفرق والأقسام وربط الموظفين بها.
- **التحقق من هوية وحضور الموظف:**
  - تسجيل آمن للحضور والانصراف عبر تطبيق الهاتف.
  - آلية تحقق متعددة الطبقات تشمل (معرف الجهاز الفريد، الموقع الجغرافي، وبصمة الوجه الحية).
  - آليات بديلة للتحضير في الحالات الاستثنائية (عبر المشرف أو يدوياً).
- **إدارة الجداول الزمنية والسياسات:**
  - إنشاء وإدارة جداول زمنية وورديات عمل مرنة.
  - تطبيق سياسات مخصصة للتأخير، الانصراف المبكر، والغياب.
- **المراقبة وإعداد التقارير:**
  - لوحة تحكم توفر نظرة شاملة وفورية على حالة حضور جميع الموظفين.
  - إنشاء وتصدير تقارير مفصلة وتحليلية لدعم اتخاذ القرارات الإدارية.
  - سجل تدقيق كامل لجميع العمليات الهامة في النظام.
- **المراقبة المستمرة للأمان:**
  - نظام للكشف عن محاولات التحايل (مثل استخدام المواقع الوهمية).
  - آلية للتحقق الدوري من تواجد الموظفين في مواقعهم أثناء ساعات العمل.

2.3. خصائص المستخدمين (User Characteristics)

سيتفاعل مع نظام الحضور الذكي أربع فئات رئيسية من المستخدمين. لكل فئة مهارات، مسؤوليات، واحتياجات مختلفة من النظام.

فئة المستخدم	التعليم والمهارات المتوقعة	المسؤوليات الرئيسية في النظام
الموظف (Employee)	- إلمام أساسي باستخدام تطبيقات الهواتف الذكية (Android/iOS).- لا يتطلب أي خبرة تقنية متخصصة.	- تسجيل الحضور والانصراف اليومي عبر تطبيق الهاتف.- عرض سجلات حضوره الشخصية.- (إذا تم تفعيلها) تقديم تبريرات للتأخير أو الغياب.

المشرف / قائد الفريق (Team Lead)	- مهارات جيدة في استخدام تطبيقات الهواتف الذكية.- قدرة على متابعة وإدارة فريق صغير.	- جميع مسؤوليات "الموظف".- تسجيل حضور أعضاء فريقه في الحالات الاستثنائية.- (مقترح) مراقبة حالة حضور فريقه المباشر.
مدير الموارد البشرية / مدير الفرع (HR Manager)	- إلمام جيد باستخدام تطبيقات الويب ومتصفحات الإنترنت.- قدرة على تحليل البيانات واستخراج التقارير.- فهم لسياسات وقوانين العمل.	- الوصول إلى لوحة التحكم لمراقبة حضور الموظفين الخاضعين لإدارته.- إنشاء وتصدير التقارير (شهرية، يومية، إلخ).- تعديل وتبرير حالات الحضور (مثل تسجيل إجازة مرضية).- إدارة العطلات الرسمية وتقويم الشركة.

مسؤول النظام (System Administrator)	- خلفية تقنية قوية وفهم جيد لإدارة الأنظمة البرمجية.- القدرة على التعامل مع الإعدادات المعقدة للنظام.	- إدارة كاملة لجميع جوانب النظام.- إضافة وتعديل حسابات جميع المستخدمين.- إدارة الهيكل التنظيمي (الفروع والفرق).- تكوين الجداول الزمنية والسياسات العامة.- مراقبة صحة النظام وأمانه، والتعامل مع أي مشاكل تقنية.

2.4. القيود العامة (General Constraints)

هذه هي القيود أو القواعد التي يجب على فريق التطوير الالتزام بها أثناء تصميم وبناء النظام.

- **C-1: المنصة (Platform):** يجب أن يعمل تطبيق الموظف على نظامي التشغيل **Android (الإصدار 8.0 أو أحدث)** و **iOS (الإصدار 13.0 أو أحدث)**.
- **C-2: لغة الواجهات (Language):** يجب أن تدعم جميع واجهات النظام (تطبيق الهاتف ولوحة التحكم) **اللغة العربية** كلغة أساسية، مع إمكانية إضافة دعم للغة الإنجليزية في المستقبل.
- **C-3: التقنيات المحددة (Technology Stack):** سيتم بناء تطبيق الهاتف باستخدام إطار العمل **Flutter** لضمان التوافق مع Android و iOS من قاعدة كود واحدة. سيتم بناء لوحة التحكم كـ **تطبيق ويب حديث (Modern Web App)**.
- **C-4: الخصوصية (Privacy):** يجب على النظام التعامل مع بيانات الموظفين، خاصة البيانات الحيوية (بصمة الوجه) والمواقع الجغرافية، بأقصى درجات السرية والأمان.
  - **C-4-1:** يجب عدم تخزين صور الوجه الخام بعد إنشاء بصمة الوجه (Faceprint)، إلا للصور الملتقطة كدليل إثبات عند عمليات التسجيل، والتي يجب أن تكون متاحة فقط للمدراء المصرح لهم.

- **C-4-2:** يجب أن تقتصر عملية تتبع الموقع الجغرافي الدوري على ساعات العمل الرسمية المحددة في جدول الموظف فقط.

- **C-5: الأمان (Security):** يجب أن تتم جميع الاتصالات بين تطبيق الهاتف والسيرفر عبر قنوات مشفرة وآمنة (**HTTPS/TLS**).

2.5. الافتراضات والاعتماديات (Assumptions and Dependencies)

يسرد هذا القسم الافتراضات التي تم وضعها أثناء كتابة المتطلبات، والظروف الخارجية التي يعتمد عليها نجاح النظام.

2.5.1. الافتراضات (Assumptions)

الافتراضات التالية تعتبر صحيحة وقد يؤثر عدم صحتها على نطاق المشروع أو جدوله الزمني:

- **A-1: توفر الأجهزة لدى الموظفين:** نفترض أن جميع الموظفين الذين سيستخدمون آلية التحضير الذاتي يمتلكون هواتف ذكية (Android أو iOS) قادرة على تشغيل التطبيق وتفي بالحد الأدنى من المتطلبات (كاميرا أمامية، خدمات الموقع، اتصال بالإنترنت).
- **A-2: توفر الاتصال بالإنترنت:** نفترض أن هواتف الموظفين ستكون متصلة بالإنترنت (عبر Wi-Fi أو بيانات الجوال) في معظم الأوقات لإتمام عمليات تسجيل الحضور والانصراف وإرسال البيانات المجمعة. (على الرغم من أن النظام سيصمم للتعامل مع انقطاعات الاتصال المؤقتة).
- **A-3: دقة خدمات الموقع:** نفترض أن خدمات تحديد المواقع (GPS) المدمجة في هواتف الموظفين توفر دقة كافية لتطبيق سياسات السياج الجغرافي.
- **A-4: التعاون الإداري:** نفترض أن إدارة الشركة ستوفر البيانات اللازمة (قوائم الموظفين، الهياكل التنظيمية، سياسات الحضور) لمسؤول النظام لإعداد النظام لأول مرة.
- **A-5: قبول المستخدمين:** نفترض أن الموظفين سيقبلون استخدام التطبيق وسيتم تدريبهم على كيفية استخدامه بشكل صحيح، بما في ذلك منح الأذونات اللازمة (للكاميرا والموقع) ليعمل التطبيق بكفاءة.

2.5.2. الاعتماديات (Dependencies)

يعتمد النظام على عدة خدمات وبنى تحتية خارجية ليعمل بشكل كامل:

- **D-1: خدمات خرائط خارجية:** يعتمد النظام على واجهة برمجة تطبيقات (API) لخدمة خرائط خارجية (مثل Google Maps أو OpenStreetMap) لعرض الخرائط في لوحة التحكم وللسماح للمسؤولين بتحديد السياج الجغرافي.
- **D-2: خدمات الإشعارات (Push Notifications):** يعتمد النظام على خدمات الإشعارات التي توفرها جوجل (Firebase Cloud Messaging - FCM) وأبل (Apple Push Notification Service - APNS) لإرسال الإشعارات إلى هواتف الموظفين.
- **D-3: البنية التحتية للاستضافة (Hosting Infrastructure):** يعتمد النظام على مزود خدمات سحابية (مثل AWS, Azure, Google Cloud) لاستضافة السيرفر وقاعدة البيانات وضمان توفرها وأدائها.

- **D-4: مكتبات الطرف الثالث (Third-party Libraries):** يعتمد تطبيق الهاتف على مكتبات مفتوحة المصدر (مثل ML Kit و TFLite) لتنفيذ وظائف التعرف على الوجه. استقرار وأداء هذه المكتبات يؤثر مباشرة على النظام.

---

3. القسم الثالث: المتطلبات المحددة (Specific Requirements)

يحتوي هذا القسم على التفاصيل الدقيقة لجميع المتطلبات التي يجب على النظام تلبيتها. هذه المتطلبات ستكون الأساس الذي سيعتمد عليه فريق التصميم والتطوير والاختبار.

3.1. متطلبات الواجهات الخارجية (External Interface Requirements)

- **UI-1: البساطة وسهولة الاستخدام: يجب تصميم جميع واجهات المستخدم (في كل من تطبيق الهاتف ولوحة التحكم) لتكون بديهية وسهلة الاستخدام، مع التركيز على تقليل عدد الخطوات اللازمة لإنجاز المهام الأساسية.**
- **UI-2: التصميم المتجاوب (Responsive Design):**
  - **UI-2.1: يجب أن تتكيف واجهة تطبيق الهاتف مع مختلف أحجام الشاشات والدقة لأجهزة Android و iOS الشائعة.**
  - **UI-2.2: يجب أن تكون لوحة التحكم المستندة إلى الويب متجاوبة، بحيث يمكن الوصول إليها واستخدامها بشكل فعال على شاشات أجهزة الكمبيوتر المكتبية والأجهزة اللوحية (Tablets).**
-
- **UI-3: دعم اللغة العربية: يجب أن تكون جميع النصوص، العناوين، الأزرار، والرسائل في واجهات المستخدم باللغة العربية، مع دعم كامل لاتجاه النص من اليمين إلى اليسار (RTL).**
- **UI-4: إرشادات واضحة للمستخدم: يجب أن يوفر النظام رسائل إرشادية ورسائل خطأ واضحة للمستخدمين. على سبيل المثال، عند فشل عملية التحقق من الوجه، يجب أن يوضح التطبيق سبب الفشل (مثل "الإضاءة ضعيفة جدًا" أو "لم يتم اكتشاف الوجه").**
- **UI-5: الهوية البصرية الموحدة: يجب أن تتبع جميع شاشات النظام هوية بصرية متسقة (Consistent Visual Identity) من حيث الألوان، الخطوط، وأسلوب تصميم الأيقونات.**
- **SI-1: واجهة برمجة تطبيقات خرائط: يجب أن يتكامل النظام مع واجهة برمجة تطبيقات (API) لخدمة خرائط خارجية (سيتم تحديدها لاحقًا، مثل Google Maps API) لتحقيق الوظائف التالية:**
  - **عرض الخرائط في لوحة التحكم.**
  - **تمكين المسؤول من تحديد ورسم السياج الجغرافي (Geofence) للمواقع والفروع.**
- **SI-2: واجهة برمجة تطبيقات الإشعارات: يجب أن يتكامل النظام مع خدمات الإشعارات الأصلية للمنصات:**
  - **SI-2.1: Firebase Cloud Messaging (FCM) لإرسال الإشعارات لأجهزة Android.**
  - **SI-2.2: Apple Push Notification Service (APNS) لإرسال الإشعارات لأجهزة iOS.**
- **SI-3: واجهة برمجة التطبيقات الداخلية (Internal API): يجب أن يتم تصميم واجهة برمجة تطبيقات (API) داخلية آمنة وموثوقة من نوع RESTful (أو GraphQL) لتسهيل الاتصال بين تطبيق الهاتف (العميل) والسيرفر.**
- **HI-1: الكاميرا الأمامية: يجب أن يكون لتطبيق الهاتف القدرة على الوصول إلى الكاميرا الأمامية للجهاز واستخدامها لالتقاط الصور اللازمة لعمليات تسجيل والتحقق من بصمة الوجه.**
- **HI-2: خدمات الموقع (GPS): يجب أن يكون للتطبيق القدرة على الوصول إلى خدمات تحديد الموقع في الجهاز للحصول على إحداثيات GPS اللازمة للتحقق من التواجد داخل السياج الجغرافي.**

- **HI-3: مستشعرات المصادقة الحيوية (Biometric Sensors): يجب أن يتكامل التطبيق مع مستشعرات بصمة الإصبع أو أنظمة التعرف على الوجه المدمجة في نظام التشغيل (مثل Face ID / Touch ID) لاستخدامها كطبقة إضافية من التحقق عند الحاجة.**
- **HI-4: الاتصال بالشبكة: يجب أن يستخدم التطبيق إمكانيات الاتصال بالشبكة في الجهاز (Wi-Fi, Cellular Data) للتواصل مع السيرفر.**

3.2. المتطلبات الوظيفية (Functional Requirements)

يحدد هذا القسم الوظائف والسلوكيات المحددة التي يجب على النظام تنفيذها. يتم تنظيم المتطلبات حسب الميزات الرئيسية للنظام.

- **FR-1.1.1: يجب أن يوفر النظام واجهة آمنة لتسجيل الدخول لجميع المستخدمين (في تطبيق الهاتف ولوحة التحكم).**
- **FR-1.1.2: يجب أن تتم عملية المصادقة باستخدام البريد الإلكتروني وكلمة المرور المسجلين للمستخدم.**
- **FR-1.1.3: يجب على النظام منع محاولات تسجيل الدخول المتكررة والخاطئة (Brute-force attacks) عن طريق قفل الحساب مؤقتًا (مثلاً، لمدة 15 دقيقة) بعد عدد معين من المحاولات الفاشلة (مثلاً، 5 محاولات).**
- **FR-1.1.4: عند تسجيل الدخول بنجاح، يجب على النظام إنشاء جلسة (Session) آمنة للمستخدم وتوجيهه إلى الواجهة الرئيسية المناسبة بناءً على دوره (Role).**
- **FR-1.2.1: يجب أن يوفر النظام آلية "نسيت كلمة المرور" للمستخدمين.**
- **FR-1.2.2: عند طلب إعادة تعيين كلمة المرور، يجب على النظام التحقق من وجود البريد الإلكتروني المدخل في قاعدة البيانات.**
- **FR-1.2.3: يجب على النظام إرسال رابط آمن ومؤقت (ينتهي صلاحيته بعد فترة قصيرة، مثلاً ساعة واحدة) إلى البريد الإلكتروني المسجل للمستخدم.**
- **FR-1.2.4: يجب أن يسمح الرابط للمستخدم بتعيين كلمة مرور جديدة تفي بسياسات تعقيد كلمة المرور.**
- **FR-1.3.1: إضافة مستخدم جديد: يجب أن يتمكن مسؤول النظام من إضافة مستخدمين جدد (من جميع الأدوار) من خلال لوحة التحكم عن طريق إدخال بياناتهم الأساسية (الاسم الكامل، الرقم الوظيفي، البريد الإلكتروني، الدور، الفرع، الفريق).**
- **FR-1.3.2: كلمة المرور الأولية: عند إنشاء حساب جديد، يجب على النظام إما إنشاء كلمة مرور عشوائية قوية وإرسالها إلى بريد الموظف، أو إرسال رابط لتعيين كلمة المرور لأول مرة.**
- **FR-1.3.3: تعديل بيانات المستخدم: يجب أن يتمكن مسؤول النظام من عرض وتعديل بيانات أي مستخدم في النظام (باستثناء كلمة المرور).**
- **FR-1.3.4: إدارة حالة الحساب: يجب أن يتمكن مسؤول النظام من تغيير حالة حساب المستخدم (نشط، معلّق، مؤرشف).**
  - **FR-1.3.4.1: المستخدمون ذوو الحالة "معلّق" لا يمكنهم تسجيل الدخول إلى النظام.**
  - **FR-1.3.4.2: المستخدمون ذوو الحالة "مؤرشف" لا يظهرون في القوائم النشطة ولكن يتم الاحتفاظ ببياناتهم التاريخية.**
- **FR-1.3.5: البحث والتصفية: يجب أن توفر لوحة التحكم لمسؤول النظام القدرة على البحث عن المستخدمين وتصفيتهم (Filter) بناءً على الاسم، الدور، الفرع، أو الحالة.**
- **FR-1.3.6: فك ارتباط الجهاز: يجب أن يتمكن مسؤول النظام من "فك ارتباط" الجهاز المحمول الحالي للموظف، مما يسمح للموظف بتسجيل الدخول وإقران جهاز جديد.**

هذه الوظائف متاحة بشكل أساسي لـ مسؤول النظام عبر لوحة التحكم.

- **FR-2.1.1: إضافة فرع جديد: يجب أن يتمكن مسؤول النظام من إضافة فرع أو موقع عمل جديد.**
- **FR-2.1.2: بيانات الفرع: عند إضافة فرع، يجب إدخال البيانات التالية كحد أدنى:**
  - **اسم الفرع (مثال: "المركز الرئيسي - الرياض").**
  - **وصف موجز (اختياري).**
  - **العنوان الفعلي.**
- **FR-2.1.3: تحديد السياج الجغرافي (Geofence):**
  - **FR-2.1.3.1: يجب أن يوفر النظام واجهة خريطة تفاعلية لتمكين المسؤول من تحديد الموقع الجغرافي الدقيق للفرع.**
  - **FR-2.1.3.2: يجب أن يتمكن المسؤول من تحديد السياج الجغرافي للفرع عن طريق تحديد نقطة مركزية ونصف قطر (Radius) بالمتر (لتشكيل دائرة).**
  - **FR-2.1.3.3: يجب عرض السياج الجغرافي بشكل مرئي على الخريطة لتسهيل عملية الضبط.**
- **FR-2.1.4: تعديل وحذف الفروع:**
  - **FR-2.1.4.1: يجب أن يتمكن مسؤول النظام من تعديل بيانات أي فرع موجود (بما في ذلك إعادة ضبط السياج الجغرافي).**
  - **FR-2.1.4.2: يجب أن يتمكن مسؤول النظام من حذف (أو أرشفة) فرع. لا يمكن حذف فرع إذا كان لا يزال هناك موظفون أو فرق مرتبطة به.**
- **FR-2.2.1: إضافة فريق جديد: يجب أن يتمكن مسؤول النظام من إضافة فريق أو قسم جديد.**
- **FR-2.2.2: ربط الفريق بالفرع: عند إضافة فريق جديد، يجب ربطه بفرع واحد موجود. (لا يمكن وجود فريق بدون فرع).**
- **FR-2.2.3: بيانات الفريق: يجب إدخال البيانات التالية كحد أدنى:**
  - **اسم الفريق (مثال: "فريق الدعم الفني").**
  - **الفرع الذي ينتمي إليه.**
- **FR-2.2.4: تعيين مشرف للفريق: يجب أن يتمكن مسؤول النظام من تعيين موظف واحد (يجب أن يكون عضوًا في هذا الفريق) كـ "مشرف" أو "قائد فريق".**
- **FR-2.2.5: تعديل وحذف الفرق:**
  - **FR-2.2.5.1: يجب أن يتمكن مسؤول النظام من تعديل بيانات أي فريق (تغيير اسمه أو الفرع التابع له).**
  - **FR-2.2.5.2: يجب أن يتمكن مسؤول النظام من حذف فريق. لا يمكن حذف فريق إذا كان لا يزال هناك موظفون مرتبطون به.**
- **FR-2.2.6: عرض هرمي: يجب أن تعرض لوحة التحكم الهيكل التنظيمي بطريقة واضحة، بحيث يمكن للمستخدم رؤية الفرق التابعة لكل فرع.**

هذه الوظائف متاحة بشكل أساسي لـ مسؤول النظام عبر لوحة التحكم.

- **FR-3.1: عرض قائمة الموظفين: يجب أن تعرض لوحة التحكم قائمة بجميع الموظفين النشطين في النظام مع بياناتهم الأساسية (الاسم، الرقم الوظيفي، الفرع، الفريق).**
- **FR-3.2: ملف الموظف الشخصي:**
  - **FR-3.2.1: يجب أن يكون لكل موظف صفحة ملف شخصي مفصلة في لوحة التحكم.**
  - **FR-3.2.2: يجب أن تعرض صفحة الملف الشخصي جميع البيانات المسجلة للموظف (المعلومات الشخصية، التنظيمية، والتقنية) التي حددناها سابقًا (الاسم، الرقم الوظيفي، البريد الإلكتروني، الدور، الفرع، الفريق، حالة الحساب، الجهاز المرتبط، الجدول الزمني المعين، إلخ).**
- **FR-3.3: ربط الموظف بالهيكل التنظيمي:**

- **FR-3.3.1: عند إضافة أو تعديل موظف، يجب على مسؤول النظام تعيين الموظف إلى فريق واحد محدد (وبالتالي، يتم تعيينه تلقائيًا إلى فرع الفريق).**
- **FR-3.3.2: يجب أن تكون عملية اختيار الفريق سهلة، بحيث يقوم المسؤول أولاً باختيار الفرع، ثم تظهر له قائمة بالفرق الموجودة داخل هذا الفرع فقط.**

- **FR-3.4: تعيين الجدول الزمني:**
  - **FR-3.4.1: يجب أن يتمكن مسؤول النظام من تعيين جدول زمني (Schedule) محدد لكل موظف من قائمة الجداول الزمنية المعرفة مسبقًا.**
  - **FR-3.4.2: يجب أن يكون هناك جدول زمني افتراضي يتم تعيينه للموظف الجديد، مع إمكانية تغييره.**
- **FR-3.5: إدارة الاستثناءات الفردية:**
  - **FR-3.5.1: يجب أن تحتوي صفحة ملف الموظف على خيار (Checkbox) لـ "السماح بالتحضير خارج الموقع"، والذي يمكن لمسؤول النظام تفعيله أو تعطيله للموظف بشكل فردي.**
- **FR-3.6: استيراد مجمع للموظفين (Bulk Import):**
  - **FR-3.6.1: لتسهيل عملية الإعداد الأولية، يجب أن يدعم النظام إمكانية استيراد قائمة من الموظفين دفعة واحدة من ملف بصيغة CSV.**
  - **FR-3.6.2: يجب أن توفر لوحة التحكم نموذج (Template) لملف CSV يمكن للمسؤول تحميله وملؤه بالبيانات الصحيحة.**
  - **FR-3.6.3: يجب على النظام التحقق من صحة البيانات في الملف أثناء عملية الاستيراد وتقديم تقرير بالأخطاء (إن وجدت)، مثل الأرقام الوظيفية المكررة أو رسائل البريد الإلكتر الإلكتروني غير الصحيحة.**
- **FR-3.7: إدارة مدراء الموارد البشرية (HR Managers):**
  - **FR-3.7.1: عند تعيين مستخدم كـ "مدير موارد بشرية"، يجب أن يتمكن مسؤول النظام من ربط هذا المدير بفرع واحد أو أكثر هو مسؤول عنه.**
  - **FR-3.7.2: صلاحيات مدير الموارد البشرية (في عرض الموظفين والتقارير) يجب أن تقتصر فقط على الموظفين الموجودين في الفروع المرتبط بها.**

تصف هذه المجموعة من المتطلبات عملية تسجيل الحضور والانصراف التي يقوم بها الموظف عبر تطبيق الهاتف، بما في ذلك جميع طبقات التحقق والأمان.

- **FR-4.1.1:** عند أول تسجيل دخول ناجح للموظف على جهاز جديد، يجب على التطبيق التقاط معرّف فريد ومستقر للجهاز (Unique and Stable Device ID).
- **FR-4.1.2:** يجب على التطبيق إرسال هذا المعرّف إلى السيرفر ليتم ربطه بشكل آمن بملف الموظف.
- **FR-4.1.3:** في كل عملية تسجيل دخول لاحقة، يجب على التطبيق إرسال معرّف الجهاز الحالي ليقوم السيرفر بالتحقق من مطابقته للمعرّف المسجل.
- **FR-4.1.4:** إذا كان معرّف الجهاز غير مطابق، يجب على النظام منع عملية تسجيل الدخول وعرض رسالة للموظف تفيد بأن حسابه مرتبط بجهاز آخر.

- **FR-4.2.1: نقطة انطلاق العملية:** يجب أن تبدأ عملية تسجيل الحضور عندما يضغط الموظف على زر مخصص في الواجهة الرئيسية للتطبيق (مثل "تسجيل حضور").
- **FR-4.2.2: سلسلة التحقق التلقائية:** عند بدء العملية، يجب على التطبيق تنفيذ سلسلة من عمليات التحقق بالتتابع. يجب أن تنجح كل خطوة للانتقال إلى الخطوة التالية.
- **FR-4.2.3: التحقق من أمان بيئة التشغيل (Security Environment Check):**
  - **FR-4.2.3.1:** يجب على التطبيق التحقق مما إذا كانت ميزة "المواقع الوهمية" (Mock Location) مفعلة. إذا كانت كذلك، يجب إيقاف العملية وإعلام الموظف بضرورة تعطيلها.
  - **FR-4.2.3.2:** يجب على التطبيق التحقق مما إذا كان الجهاز مكسور الحماية (Rooted/Jailbroken). إذا كان كذلك، يجب إيقاف العملية وعرض رسالة تحذيرية للموظف.
- **FR-4.2.4: التحقق من الموقع الجغرافي (Geofence Check):**
  - **FR-4.2.4.1:** هذا التحقق يتم فقط للموظفين الذين لم يتم منحهم استثناء "التحضير خارج الموقع".
  - **FR-4.2.4.2:** يجب على التطبيق طلب الموقع الجغرافي الحالي للجهاز بدقة عالية.
  - **FR-4.2.4.3:** يجب على التطبيق مقارنة الموقع الحالي بالسياج الجغرافي المحدد لموقع عمل الموظف (الذي تم جلبه مسبقًا من السيرفر).
  - **FR-4.2.4.4:** إذا كان الموقع خارج السياج الجغرافي، يجب إيقاف العملية وإعلام الموظف بأنه خارج منطقة العمل المسموح بها.
- **FR-4.2.5: التحقق من بصمة الوجه (Face Verification):**
  - **FR-4.2.5.1: التحقق من الحيوية (Liveness Detection):** يجب على التطبيق فتح الكاميرا الأمامية والمطالبة بإجراء بسيط (مثل الرمش) للتأكد من أن المستخدم شخص حقيقي وليس صورة.
  - **FR-4.2.5.2: التقاط الصورة واستخلاص البصمة:** بعد نجاح التحقق من الحيوية، يجب على التطبيق التقاط صورة واستخلاص بصمة الوجه الحالية (Live Faceprint) باستخدام نموذج TFLite على الجهاز.
  - **FR-4.2.5.3: المقارنة:** يجب على التطبيق مقارنة البصمة الحالية بالبصمة المرجعية (Reference Faceprint) للموظف.
  - **FR-4.2.5.4:** يجب أن تنجح المقارنة إذا كانت المسافة المحسوبة بين البصمتين أقل من "عتبة القبول" المحددة مسبقًا.
  - **FR-4.2.5.5:** إذا فشلت المقارنة، يجب إيقاف العملية وعرض رسالة خطأ واضحة للمستخدم.
- **FR-4.2.6: إتمام عملية التسجيل:**
  - **FR-4.2.6.1:** عند نجاح جميع عمليات التحقق السابقة، يجب على التطبيق إرسال طلب تسجيل الحضور إلى السيرفر.
  - **FR-4.2.6.2:** يجب أن يحتوي الطلب على: هوية الموظف، الطابع الزمني الدقيق، الموقع الجغرافي المسجل، وصورة الإثبات (السيلفي).
  - **FR-4.2.6.3:** يجب على السيرفر التحقق من الطلب وتسجيل الحضور في قاعدة البيانات.
  - **FR-4.2.6.4:** يجب أن يعرض التطبيق رسالة تأكيد نجاح العملية للموظف.

- **FR-4.3.1:** يجب أن تتبع عملية تسجيل الانصراف نفس سلسلة التحقق المطبقة في عملية تسجيل الحضور (أمان البيئة، الموقع الجغرافي، وبصمة الوجه) لضمان أن الموظف ينصرف من موقع العمل بنفسه.

- **FR-4.4.1:** يجب أن يوفر التطبيق واجهة مخصصة للموظف لتسجيل بصمة وجهه لأول مرة.

- **FR-4.4.2:** يجب على الواجهة إرشاد الموظف لالتقاط عدة صور (مثلاً، 3-5 صور) لوجهه في زوايا مختلفة قليلاً لضمان إنشاء بصمة مرجعية دقيقة.
- **FR-4.4.3:** يجب على التطبيق معالجة هذه الصور على الجهاز، استخلاص بصمة لكل صورة، ثم حساب المتوسط لإنشاء بصمة مرجعية نهائية واحدة.
- **FR-4.4.4:** يجب على التطبيق إرسال البصمة المرجعية النهائية فقط إلى السيرفر ليتم تخزينها بشكل آمن.

- **FR-4.5.1: الوصول للوظيفة:** يجب أن يظهر خيار "تحضير الفريق" في تطبيق الهاتف للمستخدمين الذين يملكون دور "مشرف" فقط.
- **FR-4.5.2: عرض قائمة الفريق:** عند اختيار هذا الخيار، يجب أن يعرض التطبيق قائمة بالموظفين الذين يقعون تحت إشراف هذا المشرف مباشرةً فقط.
- **FR-4.5.3: بدء عملية التحضير:** عند اختيار المشرف لموظف معين من القائمة لتحضيره، يجب على التطبيق تنفيذ سلسلة التحقق التالية:
  - **FR-4.5.3.1: التحقق من موقع المشرف:** يجب على التطبيق التحقق من أن الموقع الجغرافي **للمشرف** يقع ضمن السياج الجغرافي المحدد لموقع عمل الموظف المراد تحضيره.
  - **FR-4.5.3.2: التقاط صورة إثبات:** يجب على التطبيق فتح الكاميرا ومطالبة المشرف بالتقاط صورة واضحة لوجه الموظف كدليل على حضوره.
- **FR-4.5.4: إتمام عملية التسجيل:**
  - **FR-4.5.4.1:** عند نجاح التحقق والتقاط الصورة، يجب على التطبيق إرسال طلب تسجيل الحضور إلى السيرفر.
  - **FR-4.5.4.2:** يجب أن يحتوي الطلب على: هوية الموظف الذي تم تحضيره، هوية المشرف الذي قام بالعملية، الطابع الزمني، والموقع، وصورة الإثبات.
  - **FR-4.5.4.3:** يجب على السيرفر تسجيل الحضور في قاعدة البيانات مع **علامة واضحة (Flag)** تشير إلى أن هذه العملية تمت بواسطة مشرف.

- **FR-4.6.1: الوصول للوظيفة:** يجب أن تتوفر إمكانية إضافة سجل حضور/انصراف يدوي في **لوحة التحكم** للمستخدمين الذين يملكون صلاحيات "مسؤول نظام" أو "مدير موارد بشرية".
- **FR-4.6.2: تحديد الهدف:** يجب أن يتمكن المدير من اختيار الموظف والتاريخ والوقت المحددين لتسجيل الحضور أو الانصراف.
- **FR-4.6.3: إجبارية تسجيل السبب:** يجب أن يكون حقل "سبب التعديل اليدوي" **إلزاميًا**. لا يمكن حفظ السجل بدونه. (مثال: "عطل في هاتف الموظف").
- **FR-4.6.4: إتمام عملية التسجيل:**
  - **FR-4.6.4.1:** عند الحفظ، يجب على السيرفر إضافة سجل الحضور/الانصراف إلى قاعدة البيانات.
  - **FR-4.6.4.2:** يجب على السجل أن يحتوي على **علامة واضحة** تشير إلى أنه "تسجيل يدوي".
  - **FR-4.6.4.3:** يجب أن يتم تسجيل هوية المدير الذي قام بالإدخال اليدوي والسبب الذي قدمه في سجل التدقيق (Audit Log) بشكل دائم.

تصف هذه المجموعة من المتطلبات كيفية قيام النظام بمعالجة بيانات الحضور الخام، وتصنيفها إلى حالات مفهومة، وعرضها في تقارير مفيدة للإدارة.

- **FR-6.1.1: التصنيف الآلي:** في نهاية كل يوم عمل، يجب على النظام معالجة سجلات الحضور لكل موظف ومقارنتها بالجدول الزمني والسياسات المعينة له لتحديد **الحالة الآلية** لليوم.
- **FR-6.1.2: قائمة الحالات الآلية:** يجب أن يدعم النظام الحالات الآلية التالية كحد أدنى:
  - حاضر (On-Time)
  - متأخر (Late)
  - غائب (Absent)
  - انصراف مبكر (Early Departure)
  - وقت إضافي (Overtime)
  - يوم عطلة (Day Off) (للإجازات الأسبوعية أو الرسمية).
-
- **FR-6.1.3: إدارة الحالات اليدوية (Manual Status Management):**
  - **FR-6.1.3.1:** يجب أن يتمكن مدير الموارد البشرية (أو المشرف) من تعديل الحالة الآلية ليوم معين لموظف.
  - **FR-6.1.3.2:** يجب أن توفر الواجهة قائمة بالحالات اليدوية المعتمدة، مثل:
    - إجازة سنوية (Annual Leave)
    - إجازة مرضية (Sick Leave)
    - مهمة عمل خارجية (Business Trip)
    - غياب مبرر (Justified Absence)
    - غياب غير مبرر (Unjustified Absence)
  - **FR-6.1.3.3:** عند تغيير الحالة يدويًا، يجب تسجيل هوية المدير والوقت والسبب في سجل التدقيق.
-
- **FR-6.2.1: لوحة التحكم الرئيسية:** يجب أن توفر لوحة التحكم الرئيسية لمدير الموارد البشرية نظرة عامة وفورية على حالة الحضور لليوم الحالي.
- **FR-6.2.2: ملخص إحصائي:** يجب أن تعرض لوحة التحكم ملخصًا إحصائيًا، مثل: (إجمالي الموظفين، عدد الحاضرين، عدد المتأخرين، عدد الغائبين).
- **FR-6.2.3: قائمة الحضور الحية:** يجب أن تعرض لوحة التحكم قائمة قابلة للبحث والتصفية تظهر حالة كل موظف لليوم الحالي (مع وقت الحضور/الانصراف الفعلي).
- **FR-6.2.4: عرض سجلات الموظف:** يجب أن يتمكن المدير من النقر على أي موظف لعرض سجل حضوره التاريخي الكامل.
- **FR-6.3.1: إنشاء التقارير:** يجب أن توفر لوحة التحكم وحدة مخصصة لإنشاء التقارير.
- **FR-6.3.2: تقرير الحضور الشهري (Monthly Attendance Report):**
  - **FR-6.3.2.1:** يجب أن يكون هذا التقرير هو التقرير الرئيسي.
  - **FR-6.3.2.2:** يجب أن يسمح للمدير بتحديد النطاق الزمني (من تاريخ إلى تاريخ) والموظفين (موظف واحد، فريق، فرع، أو الكل).
  - **FR-6.3.2.3:** يجب أن يعرض التقرير ملخصًا لكل موظف خلال الفترة المحددة، يشمل: (عدد أيام العمل، عدد أيام الحضور، عدد أيام الغياب، إجمالي دقائق التأخير، إجمالي ساعات العمل الإضافي).
-
- **FR-6.3.3: تقرير الحضور اليومي المفصل (Daily Detailed Report):** يجب أن يوفر النظام تقريرًا يعرض جميع حركات الحضور والانصراف لجميع الموظفين في يوم محدد.
- **FR-6.3.4: تصدير التقارير:**
  - **FR-6.3.4.1:** يجب أن تكون جميع التقارير قابلة للتصدير.
  - **FR-6.3.4.2:** يجب أن يدعم النظام التصدير بصيغة **CSV** و **PDF** كحد أدنى.

تصف هذه المجموعة من المتطلبات أنواع الإشعارات التلقائية التي يجب على النظام إرسالها إلى مختلف فئات المستخدمين لإبقائهم على اطلاع بالأحداث المهمة.

- **FR-7.1.1: قناة الإرسال:** يجب إرسال الإشعارات الموجهة للموظفين والمشرفين كـ **إشعارات دفع (Push Notifications)** إلى تطبيق الهاتف.
- **FR-7.1.2: إعدادات الإشعارات:** يجب أن يوفر تطبيق الهاتف صفحة إعدادات تسمح للمستخدم بالتحكم في استلام الإشعارات غير الإلزامية.
- **FR-7.2.1: تذكير بتسجيل الحضور:** يجب على النظام إرسال إشعار تذكير للموظف قبل وقت بدء دوامه المحدد (يمكن تكوين المدة، مثلاً 5 دقائق).
- **FR-7.2.2: تذكير بتسجيل الانصراف:** يجب على النظام إرسال إشعار تذكير للموظف في وقت انتهاء دوامه المحدد.
- **FR-7.2.3: تأكيد العمليات:** يجب إرسال إشعار فوري للموظف لتأكيد نجاح عمليات تسجيل الحضور والانصراف.
- **FR-7.2.4: إشعار بتعديل الحالة:** يجب إرسال إشعار للموظف عندما يقوم مديره بتعديل حالة حضوره لأي يوم (مثلاً، تغييرها إلى "إجازة مرضية").
- **FR-7.2.5: إشعار بطلب التبرير:** (مرتبط بـ FR-8) يجب إرسال إشعار فوري للموظف إذا تم اكتشاف تواجده خارج موقع العمل، ليطالبه بتقديم تبرير.
- **FR-7.3.1: إشعار بتأخر عضو في الفريق:** يجب إرسال إشعار للمشرف إذا لم يقم أحد أعضاء فريقه بتسجيل الحضور بعد انتهاء فترة السماح.
- **FR-7.3.2: إشعار بطلب تبرير جديد:** يجب إرسال إشعار للمدير/المشرف عندما يقدم أحد الموظفين تبريرًا لتأخير أو مخالفة تواجد.
- **FR-7.3.3: إشعار موجز (Digest Notification):** (اختياري) يمكن للنظام إرسال ملخص يومي عبر البريد الإلكتروني إلى مدراء الموارد البشرية يحتوي على إحصائيات الحضور لليوم.
- **FR-7.4.1: إشعار أمني:** يجب إرسال إشعار (عبر البريد الإلكتروني أو في لوحة التحكم) إلى مسؤول النظام عند اكتشاف محاولة تحايل أمني خطيرة (مثل اكتشاف متكرر لاستخدام موقع وهمي من قبل مستخدم معين).
- **FR-7.4.2: إشعار بصحة النظام:** يجب على النظام إرسال تنبيهات لمسؤول النظام في حالة حدوث أخطاء حرجة في النظام (مثل عدم القدرة على الاتصال بقاعدة البيانات).

تصف هذه المجموعة من المتطلبات الميزة الأمنية التي تهدف إلى التأكد من بقاء الموظفين المقيدين بموقع في منطقة عملهم المحددة خلال ساعات الدوام.

- **FR-8.1.1: التفعيل:** يجب تفعيل هذه الآلية تلقائيًا على تطبيق الموظف فور تسجيله للدخول بنجاح، وذلك فقط للموظفين المقيدين بموقع عمل.
- **FR-8.1.2: الجدولة المحلية:** يجب على التطبيق جدولة مهمة للعمل في الخلفية بشكل دوري (سيتم تحديد الفاصل الزمني، مثلاً كل ساعة) خلال ساعات العمل الرسمية للموظف.
- **FR-8.1.3: استثناء فترة الراحة:** يجب على آلية الجدولة أن تتجنب إجراء أي تحقق خلال فترة الراحة المحددة في جدول الموظف الزمني.
- **FR-8.1.4: التنفيذ المحلي:** عند تنفيذ المهمة في الخلفية، يجب على التطبيق:
  - الحصول على الموقع الجغرافي الحالي.
  - التحقق من أمان الموقع (ضد المواقع الوهمية).

- مقارنة الموقع بالسياج الجغرافي المخزن محليًا.

- **FR-8.1.5: التخزين المحلي:** يجب على التطبيق تخزين نتيجة كل عملية تحقق (سواء OK أو VIOLATION) في قاعدة بيانات محلية مع طابع زمني دقيق.
- **FR-8.1.6: الإرسال المجمع (Batching):** يجب على التطبيق تجميع سجلات التحقق الدورية وإرسالها دفعة واحدة إلى السيرفر على فترات زمنية محددة (مثلاً، مرتين في اليوم) لتقليل استدعاءات الشبكة.
- **FR-8.1.7: الإرسال الفوري للمخالفات:** في حالة اكتشاف مخالفة (VIOLATION)، يجب على التطبيق إرسال تنبيه فوري إلى السيرفر لبدء عملية التصعيد، بالإضافة إلى تسجيلها محليًا.
- **FR-8.2.1: التحدي العشوائي (Randomized Challenge):**
  - **FR-8.2.1.1:** يجب على السيرفر، على فترات زمنية عشوائية، اختيار نسبة صغيرة من الموظفين النشطين وإرسال "طلب تحقق فوري" عبر إشعار دفع صامت.
  - **FR-8.2.1.2:** يجب على التطبيق، عند استلام هذا الإشعار، الاستجابة فورًا بموقعه الحالي.
  - **FR-8.2.1.3:** إذا فشل التطبيق في الاستجابة خلال فترة زمنية محددة، يجب على السيرفر تسجيل ذلك كـ "علامة حمراء" محتملة (تطبيق غير نشط أو تم تعطيله).

- **FR-8.2.2: التحقق من صحة السلاسل الزمنية:** عند استلام دفعة السجلات المجمعة من التطبيق، يجب على السيرفر تحليلها للبحث عن أي فجوات زمنية غير مبررة بين عمليات التحقق، والتي قد تشير إلى توقف التطبيق عن العمل لفترة.
- **FR-8.3.1:** عند استلام السيرفر لتنبيه مخالفة، يجب عليه تسجيل الحادثة فورًا في سجل الموظف.
- **FR-8.3.2:** يجب على السيرفر إرسال إشعار فوري للموظف يطالبه بتقديم تبرير للمخالفة من خلال التطبيق.
- **FR-8.3.3:** يجب على النظام عرض تنبيه في لوحة تحكم المدير/المشرف المسؤول، يعرض تفاصيل المخالفة والتبرير الذي قدمه الموظف (إن وجد).
- **FR-8.3.4:** يجب أن يتمكن المدير من "قبول" أو "رفض" التبرير.
- **FR-8.3.5:** يجب أن تكون نتيجة المخالفة (في حالة الرفض) قابلة للتكوين في إعدادات النظام (مثلاً، تسجيل علامة مخالفة، خصم من الراتب، أو اعتبار اليوم غيابًا).

تصف هذه المجموعة من المتطلبات وظائف النظام المتعلقة بتسجيل الأنشطة الهامة وتوفير آليات أمان أساسية.

- **FR-9.1.1: تسجيل الأحداث الهامة:** يجب على النظام تسجيل جميع الأحداث والعمليات الحساسة التي تتم من قبل المستخدمين في سجل تدقيق مفصل.
- **FR-9.1.2: محتوى سجل الحدث:** يجب أن يتضمن كل إدخال في سجل التدقيق كحد أدنى:
  - الطابع الزمني الدقيق للحدث.
  - هوية المستخدم الذي قام بالحدث (User ID).
  - عنوان IP الذي صدر منه الطلب.
  - وصف للحدث (مثال: "قام المستخدم admin@company.com بتعديل حالة حضور الموظف EMP-101 ليوم 2023-10-25 إلى 'إجازة مرضية'").
  - البيانات قبل وبعد التغيير (إن وجدت).

- **FR-9.1.3: قائمة الأحداث المطلوب تسجيلها:** يجب تسجيل الأحداث التالية على الأقل:
  - عمليات تسجيل الدخول (الناجحة والفاشلة).
  - أي عملية إضافة، تعديل، أو حذف للمستخدمين، الفروع، الفرق، أو الجداول الزمنية.
  - أي عملية تسجيل حضور/انصراف يدوية (Manual Entry).
  - أي تعديل على حالة حضور موظف (مثلاً، تغيير "غائب" إلى "إجازة").
  - فك ارتباط جهاز موظف.
  - تغيير كلمة المرور.
- **FR-9.1.4: الحماية من التغيير:** يجب تصميم سجل التدقيق ليكون للقراءة فقط (Read-only) وغير قابل للتعديل أو الحذف، حتى من قبل مسؤول النظام، لضمان نزاهة البيانات.
- **FR-9.1.5: واجهة عرض السجل:** يجب أن توفر لوحة التحكم واجهة خاصة لمسؤول النظام لعرض سجلات التدقيق، مع إمكانية البحث والتصفية حسب المستخدم، الحدث، أو النطاق الزمني.

- **FR-9.2.1: سياسة التعقيد:** يجب على النظام فرض سياسة لتعقيد كلمة المرور (مثلاً، طول لا يقل عن 8 أحرف، تحتوي على حروف كبيرة، صغيرة، أرقام، ورموز).
- **FR-9.2.2: التخزين الآمن:** يجب عدم تخزين كلمات المرور كنص صريح (Plain Text). يجب تجزئتها وتمليحها (Hashed and Salted) باستخدام خوارزمية حديثة وقوية (مثل bcrypt).
- **FR-9.2.3: انتهاء صلاحية كلمة المرور:** (اختياري، قابل للتكوين) يمكن للنظام أن يطلب من المستخدمين تغيير كلمات مرورهم بشكل دوري (مثلاً، كل 90 يومًا).

3.3. المتطلبات غير الوظيفية (Non-Functional Requirements - NFRs)

يحدد هذا القسم معايير الجودة والخصائص التشغيلية للنظام. هذه المتطلبات تصف "كيف" يجب أن يكون النظام، بدلاً من "ماذا" يجب أن يفعل.

- **PERF-1: زمن استجابة واجهة برمجة التطبيقات (API Response Time):** يجب أن تستجيب معظم استدعاءات واجهة برمجة التطبيقات (API) التي لا تتضمن عمليات معقدة في أقل من **500 مللي ثانية**.
- **PERF-2: زمن استجابة تطبيق الهاتف:**
  - **PERF-2.1:** يجب أن تكتمل عملية التحقق من بصمة الوجه على الجهاز (On-device) في أقل من **ثانيتين** على الأجهزة المتوسطة المواصفات.
  - **PERF-2.2:** يجب ألا يستغرق الانتقال بين الشاشات الرئيسية في تطبيق الهاتف أكثر من **ثانية واحدة**.
-
- **PERF-3: زمن تحميل لوحة التحكم:** يجب تحميل لوحة التحكم الرئيسية (Dashboard) وعرض البيانات الأولية في أقل من **3 ثوانٍ** في ظل ظروف شبكة عادية.
- **PERF-4: التعامل مع الحمل (Load Handling):** يجب أن يكون النظام قادرًا على التعامل مع ذروة الاستخدام، حيث يقوم **25%** من إجمالي الموظفين بتسجيل الحضور في نفس الفترة الزمنية (نافذة 15 دقيقة) دون تدهور ملحوظ في الأداء.

- **SEC-1: تشفير الاتصالات:** يجب أن تتم جميع الاتصالات بين تطبيق الهاتف والسيرفر، وبين متصفح المستخدم ولوحة التحكم، عبر بروتوكول **HTTPS/TLS** لمنع التنصت على البيانات.
- **SEC-2: الحماية من الثغرات الشائعة:** يجب تأمين تطبيق الويب ضد الثغرات الأمنية الشائعة المذكورة في OWASP Top 10، بما في ذلك على سبيل المثال لا الحصر:
  - الحقن (Injection)، خاصة SQL Injection.
  - البرمجة عبر المواقع (Cross-Site Scripting - XSS).
  - تزوير الطلبات عبر المواقع (Cross-Site Request Forgery - CSRF).
- **SEC-3: إدارة الجلسات الآمنة:** يجب أن يستخدم النظام آليات آمنة لإدارة جلسات المستخدمين (مثل استخدام Tokens آمنة مثل JWT) مع تحديد فترة صلاحية معقولة للجلسة.
- **SEC-4: تفويض الصلاحيات (Authorization):** يجب على السيرفر التحقق من صلاحيات المستخدم مع كل طلب API للتأكد من أن المستخدم لديه الإذن الكافي لتنفيذ العملية المطلوبة (لا يتم الاعتماد على التحقق من جانب العميل فقط).

- **REL-1: الإتاحة (Availability):** يجب أن تكون خدمات السيرفر (API وقاعدة البيانات) متاحة وقابلة للوصول بنسبة **99.5%** من الوقت، باستثناء فترات الصيانة المجدولة.
- **REL-2: التعامل مع انقطاع الشبكة:**
  - **REL-2.1:** يجب أن يتمكن تطبيق الهاتف من التعامل برشاقة مع انقطاع الاتصال المؤقت بالإنترنت.
  - **REL-2.2:** يجب أن يقوم التطبيق بتخزين العمليات الهامة التي لم يتم إرسالها (مثل سجلات التحقق الدوري) محليًا وإعادة محاولة إرسالها تلقائيًا عند عودة الاتصال.
- **REL-3: سلامة البيانات (Data Integrity):** يجب على النظام ضمان سلامة البيانات من خلال استخدام قيود قاعدة البيانات (مثل المفاتيح الخارجية) والتحقق من صحة البيانات (Validation) على جانب السيرفر قبل حفظها.
- **REL-4: النسخ الاحتياطي والاسترداد (Backup and Recovery):** يجب وضع خطة لأخذ نسخ احتياطية منتظمة (يومية على الأقل) لقاعدة البيانات، مع وجود آلية واضحة لاستعادة البيانات في حالة حدوث كارثة.

- **USA-1: الحد الأدنى من التدريب:** يجب تصميم واجهات المستخدم لتكون بديهية بما يكفي بحيث يتمكن المستخدمون غير التقنيين (خاصة الموظفين ومدراء الموارد البشرية) من أداء مهامهم الأساسية دون الحاجة إلى تدريب رسمي ومكثف.
- **USA-2: الاتساق (Consistency):** يجب أن يكون سلوك وتصميم العناصر المتشابهة متسقًا عبر جميع شاشات النظام. (مثلاً، يجب أن يكون شكل ومكان زر "حفظ" هو نفسه في كل الصفحات).
- **USA-3: التغذية الراجعة للمستخدم (User Feedback):** يجب أن يوفر النظام تغذية راجعة مرئية وفورية استجابةً لإجراءات المستخدم. (مثلاً، عرض مؤشر تحميل عند إجراء عملية تستغرق وقتًا، أو رسالة تأكيد بعد نجاح الحفظ).

- **MAIN-1: معايير الترميز (Coding Standards):** يجب أن يتبع كود المصدر معايير الترميز وأفضل الممارسات المتفق عليها للغات وأطر العمل المستخدمة (Flutter, Dart, etc.).
- **MAIN-2: التوثيق داخل الكود (Code Documentation):** يجب توثيق الأجزاء المعقدة والحاسمة من الكود المصدر بشكل جيد من خلال التعليقات لشرح الغرض منها وكيفية عملها.

- **MAIN-3: التصميم النمطي (Modularity):** يجب تصميم بنية النظام لتكون نمطية (Modular)، بحيث يمكن تعديل أو تحديث أجزاء من النظام (مثل آلية التحقق من الوجه) بأقل تأثير ممكن على الأجزاء الأخرى.

3.4. متطلبات قاعدة البيانات (Database Requirements)

يحدد هذا القسم المتطلبات المتعلقة بتخزين وإدارة البيانات في قاعدة بيانات النظام.

- **DB-1: نوع قاعدة البيانات:** يجب استخدام نظام إدارة قواعد بيانات علائقي (Relational Database Management System - RDBMS) حديث وموثوق (مثل PostgreSQL أو MySQL) لضمان اتساق وسلامة البيانات.
- **DB-2: سياسة الاحتفاظ بالبيانات (Data Retention Policy):**
  - **DB-2.1:** يجب الاحتفاظ بسجلات الحضور والانصراف التفصيلية للموظفين لمدة لا تقل عن **سنتين (2 years)** في قاعدة البيانات النشطة لتكون متاحة للتقارير الفورية.
  - **DB-2.2:** بعد انقضاء هذه المدة، يمكن أرشفة البيانات القديمة في حل تخزين طويل الأمد.
  - **DB-2.3:** يجب الاحتفاظ ببيانات سجل التدقيق (Audit Log) لمدة لا تقل عن **سبع سنوات (7 years)** أو حسب ما تقتضيه السياسات التنظيمية.
-
- **DB-3: أرشفة بيانات الموظفين:** عند تغيير حالة حساب الموظف إلى "مؤرشف" (بعد مغادرته للشركة)، يجب عدم حذف بياناته أو سجلات حضوره التاريخية من قاعدة البيانات لضمان سلامة التقارير القديمة.

---

4. الملاحق (Appendices)

- **الملحق أ: مخطط نموذج البيانات المبدئي (Initial Data Model - ERD)**
- **الملحق ب: مخططات حالات الاستخدام الرئيسية (Key Use Case Diagrams)**

(ملاحظة: هذه الملاحق سيتم إعدادها في مرحلة التصميم، ولكننا نشير إليها هنا في المستند).

القسم 5: خطة تنفيذ المشروع (Project Implementation Plan)

منهجية العمل (Development Methodology)

لضمان تحقيق التوازن بين سرعة تسليم القيمة، جودة المنتج، وإدارة الميزانية بفعالية، سيتبع المشروع منهجية تطوير مرنة ومرحلية (Agile Phased Approach). سيتم تقسيم العمل إلى ثلاث مراحل رئيسية، تبدأ بإطلاق نسخة أولية قابلة للاستخدام (MVP)،

تليها إضافة الميزات المتقدمة، وتنتهي بالإطلاق الكامل للنظام بعد اختبار شامل. هذه المنهجية تقلل من المخاطر وتسمح بجمع الملاحظات مبكرًا وتضمن أن المنتج النهائي يلبي احتياجات العمل الفعلية.

5.1. معايير النجاح والعلاقة بين الوقت، التكلفة، والجودة (Success Criteria: The Relationship Between (Time, Cost, and Quality

لضمان نجاح هذا المشروع وتحقيق أهدافه، من الضروري فهم العلاقة المترابطة بين ثلاثة معايير أساسية:

1. **الوقت (Time):** الجدول الزمني المقترح لإنجاز المشروع.
2. **التكلفة (Cost):** الميزانية المخصصة للمشروع، والتي تتمثل بشكل أساسي في حجم وخبرة فريق العمل.
3. **الجودة والنطاق (Quality & Scope):** مدى اكتمال الميزات الموثقة في هذا المستند ومستوى جودتها واستقرارها.

هذه المعايير الثلاثة مترابطة بشكل وثيق؛ **لا يمكن تغيير أحدها دون التأثير على واحد على الأقل من المعيارين الآخرين.**

بناءً على ذلك، نقدم الخيارات التالية لمتخذي القرار لاختيار المسار الذي يناسب أولويات الشركة الاستراتيجية:

- **الخيار أ (المقترح والمتوازن):** تنفيذ الخطة المقترحة (فريق من 3 مطورين وقائد، في 4-5 أشهر). هذا الخيار يوفر أفضل توازن بين **تكلفة معقولة، جدول زمني جيد، وأعلى مستوى من الجودة** لجميع الميزات.
- **الخيار ب (الأسرع تنفيذًا):** يمكننا تقصير المدة الزمنية للمشروع بشكل كبير (على سبيل المثال، إنجازه في 3 أشهر). يتطلب هذا المسار **زيادة التكلفة** عن طريق إضافة مطورين متخصصين آخرين للفريق لتسريع وتيرة العمل بالتوازي، مع الحفاظ على نفس مستوى الجودة.
- **الخيار ج (الأقل تكلفة أولية):** يمكن تنفيذ المشروع بتكلفة أولية أقل من خلال تقليل عدد المطورين في الفريق. لكن هذا سيؤدي حتمًا إلى **زيادة المدة الزمنية** للمشروع، أو قد يتطلب **تقليل نطاق الميزات** في النسخة الأولى (التضحية ببعض الجودة أو الوظائف المتقدمة) لتحقيق الإطلاق في وقت معقول.

نحن على أتم الاستعداد لمناقشة هذه الخيارات بالتفصيل لاختيار المسار الذي يحقق أهداف الشركة على أفضل وجه.

5.2. هيكل الفريق المقترح (Proposed Team Structure)

لإنجاز المشروع ضمن الجدول الزمني المقترح، نقترح فريق عمل متخصص وفعال يتكون من:

- **1x قائد فريق / مدير منتج :** مسؤول عن الرؤية الاستراتيجية، إدارة المهام، ضمان الجودة، والتواصل مع أصحاب المصلحة.
- **1x مطور واجهة خلفية (Backend Developer):** مسؤول عن بناء وتأمين السيرفر، قاعدة البيانات، وواجهة برمجة التطبيقات (API).
- **1x مطور تطبيقات فلاتر (Flutter Developer):** مسؤول عن تطوير تطبيق الهاتف (Android & iOS) بجميع وظائفه.
- **1x مطور واجهة أمامية (Frontend Developer):** مسؤول عن تطوير لوحة التحكم المستندة إلى الويب.

بالإضافة إلى:

- **1x مصمم واجهات وتجربة المستخدم (UI/UX Designer):** سيعمل بشكل جزئي (تعاقد) خلال **الشهر الأول** من المشروع، وتكون مسؤولياته الرئيسية هي:
  - تصميم الهوية البصرية للنظام.
  - إنشاء نماذج أولية (Wireframes) وواجهات تصميم نهائية (Mockups) لتطبيق الهاتف ولوحة التحكم.
  - تسليم أصول التصميم لفريق التطوير.
-

5.3. خطة التطوير المرحلية (Phased Development Plan)

المرحلة الأولى: إطلاق النسخة التجريبية (MVP/Beta) - (المدة: 2 - 2.5 شهراً)

- **الهدف:** إطلاق نسخة وظيفية ومستقرة تحل المشكلة الأساسية وتوفر قيمة فورية للشركة.
- **الميزات الرئيسية في هذه المرحلة:**
  - نظام كامل لإدارة المستخدمين، الأدوار، الفروع، والفرق.
  - آلية التحضير الذاتي للموظف باستخدام: **معرف الجهاز + الموقع الجغرافي + التقاط صورة سيلفي** (كدليل إثبات للمراجعة اليدوية في هذه المرحلة).
  - آليات التحضير عبر المشرف والتحضير اليدوي من قبل الإدارة.
  - نظام كامل لإدارة الجداول الزمنية والسياسات الأساسية.
  - لوحة تحكم لعرض بيانات الحضور الحية.
  - إنشاء وتصدير تقرير الحضور الشهري الأساسي.

المرحلة الثانية: تطوير الميزات المتقدمة - (المدة: 1.5 شهرًا)

- **الهدف:** بناء الميزات المتقدمة التي تمثل القوة التنافسية للنظام، ويتم ذلك بالتوازي مع استخدام الشركة للنسخة التجريبية.
- **الميزات الرئيسية في هذه المرحلة:**
  - تطوير وتفعيل آلية **التعرف الآلي على الوجه (Face Recognition)** ودمجها في عملية التحضير.
  - تطوير وتفعيل **آلية التحقق الدوري من التواجد** الآمنة.
  - تطوير نظام الإشعارات الكامل لجميع فئات المستخدمين.
  - تطوير تقارير إضافية وتحليلية في لوحة التحكم.

المرحلة الثالثة: الاختبار المكثف والإطلاق الرسمي - (المدة: 1 شهر)

- **الهدف:** ضمان استقرار وجودة النظام بأعلى المعايير، وجمع الملاحظات من المرحلة التجريبية، وإطلاق النسخة الكاملة.
- **الأنشطة الرئيسية في هذه المرحلة:**
  - اختبار شامل ومتكامل للنظام (End-to-end Testing).
  - إصلاح جميع الأخطاء وتحسين الأداء.
  - نشر التطبيق النهائي على متاجر Google Play و Apple App Store.
  - إعداد الوثائق النهائية وتدريب المستخدمين.

5.4. الجدول الزمني التقديري للمشروع (High-Level Timeline)

النشاط / الشهر	الشهر 1	الشهر 2	الشهر 3	الشهر 4	الشهر 5
تصميم UI/UX	[redacted]				
تطوير الواجهة الخلفية	[redacted]	[redacted]	[redacted]	[redacted]	
تطوير تطبيق فلاتر	[redacted]	[redacted]	[redacted]	[redacted]	
تطوير لوحة التحكم	[redacted]	[redacted]	[redacted]	[redacted]	
التكامل والاختبار والنشر				[redacted]	[redacted]
المرحلة المنجزة	**المرحلة 1 (MVP)**	**المرحلة 2**	**المرحلة 3**		