



جمهوری اسلامی ایران
وزارت تعاون، کار و رفاه اجتماعی

بسمه تعالی

شماره:.....

تاریخ:.....

پیوست:.....

"معاونت توسعه مدیریت و منابع"

موضوع استعلام بهاء :

تامین و پشتیبانی سرویس ارسال پیامک

شرایط عمومی و شرح خدمات

اداره کل پشتیبانی

اداره امور قراردادها



جمهوری اسلامی ایران

وزارت تعاون، کار و رفاه اجتماعی

شرایط عمومی

بسم تعالی

شماره:.....

تاریخ:.....

پیوست:.....

الف - اسناد، مدارک و سوابق شرکت:

- ارائه گواهینامه ها و تاییدیه های مورد نیاز اشاره شده در شرح خدمات که در زمان انعقاد قرارداد معتبر بوده و برنده استعلام بهاء مکلف به تمدید آن تا پایان قرارداد خواهد بود.
- ارائه پرینت تاییدیه ثبت نام در سامانه ثنا (قوه قضائیه)
- ارائه گواهی عدم مداخله کارکنان دولت در معاملات دولتی (متقاضی اقرار نماید که مشمول منع مداخله کارکنان دولت نمی باشد)
- تصویر اساسنامه، روزنامه رسمی و آخرین تغییرات شرکت (صاحبان مجاز امضاء).
- ارائه شناسه ملی و کد اقتصادی.
- ارائه گواهی ثبت نام مالیات بر ارزش افزوده که ضروری است و برنده استعلام بهاء موظف به تمدید اعتبار آن تا پایان قرارداد می باشد. (پرداخت مالیات بر ارزش افزوده در صورت ارائه گواهی مورد اشاره بعهدہ دستگاه می باشد)
- ارائه رزومه و سوابق کاری شرکت به همراه فتوکپی از صفحات اول و توضیحات شناسنامه مدیرعامل و اعضای که حق امضاء تعهدآور دارند.

- تکمیل جدول ذیل:

۱- اسامی صاحبان مجاز امضاء اسناد تعهدآور و قراردادهای مطابق با آخرین روزنامه رسمی کشور (با نمونه امضاء):		
نام و نام خانوادگی:	کد ملی:	تاریخ تولد:
نام و نام خانوادگی:	کد ملی:	تاریخ تولد:
۲- شماره و تاریخ ثبت:		
۳- شماره و تاریخ تعیین صلاحیت و مجوز فعالیت:		
۴- شناسه ملی:		
۵- کد اقتصادی:		
۶- شماره و تاریخ روزنامه رسمی آخرین تغییرات در امضاء های مجاز:		
۷- شماره کد کارگاهی دریافتی از سازمان تامین اجتماعی:		
۸- آدرس، کدپستی و شماره تلفن:		
۹- شماره حساب و شبا (ترجیحاً بانک ملی):		
۱۰- نام و شماره تلفن نماینده جهت هماهنگی لازم:		
نام:	تلفن همراه:	شماره تلفن ثابت:



جمهوری اسلامی ایران

وزارت تعاون، کار و رفاه اجتماعی

بسمه تعالی

شماره:.....

تاریخ:.....

پیوست:.....

ب - سایر شرایط:

- ۱- مدت زمان انجام کار از تاریخ عقد قرارداد لغایت پایان سال مالی می باشد.
- ۲- کسورات قانونی شامل: مالیات، بیمه تأمین اجتماعی، تضمین، سپرده حسن انجام کار و همچنین دریافت مفاصا حساب از بیمه بر عهده پیمانکار خواهد بود.
- ۳- اسناد شرایط عمومی و شرح خدمات جزء لاینفک قرارداد محسوب خواهد شد.
- ۴- با توجه به مراحل بررسی و نحوه رسیدگی به اسناد دریافتی از شرکت کنندگان، طبق قوانین و مقررات و پس از تایید مدارک مورد اشاره، مناسب ترین قیمت پیشنهادی انتخاب و به وی ابلاغ خواهد شد.
- ۵- برنده موظف است حداکثر ظرف مدت ۲روز از زمان اعلام برنده توسط دستگاه، نسبت به پذیرش یا عدم پذیرش برنده بودن خود در سامانه تدارکات الکترونیکی دولت اقدام نماید.
- ۶- پیمانکار مکلف به رعایت آئین نامه تضمین برای معاملات دولتی به شماره ۱۲۳۴۰۲/ت ۵۰۶۵۹ ه مورخ ۹۴/۰۹/۲۲ خواهد بود.
- ۷- بارگذاری جدول آنالیز قیمت در سامانه الزامی می باشد.

➤ توضیحات:

- شرکت کنندگان می بایست کلیه اوراق و اسناد استعلام بهاء شامل: شرایط عمومی، شرح خدمات (بارگذاری شده در فیلد مدارک پیوستی در صفحه اعلان عمومی نیاز) و اسناد و مدارک شرکت کننده (ذکر شده در شرایط عمومی و شرح خدمات) را بدون تغییر به امضاء صاحبان مجاز و ممهور به مهر تأمین کننده رسانده و در قسمت مدارک پیوستی در سامانه تدارکات الکترونیکی دولت تا پایان مهلت ارسال پاسخ بارگذاری نمایند (بارگذاری مدارک می

بایست در قالب یک فایل با فرمت PDF انجام شود)

- شرکت کنندگان در صورت داشتن ابهام در شرح خدمات با شماره تلفن ۶۴۴۹۲۷۱۲ خانم تیموری و آقای فیروزی و شرایط عمومی با شماره تلفن ۶۴۴۹۲۶۲۶ تماس حاصل نمایند .
- کلیه مدارک می بایست به صورت خوانا و شفاف، تهیه و ارائه شود.
- تذکر: در صورت عدم بارگذاری مدارک ذکر شده در شرایط عمومی و شرح خدمات از سوی شرکت کننده، قیمت پیشنهادی بارگذاری شده ابطال می گردد.



جمهوری اسلامی ایران وزارت تعاون، کار و رفاه اجتماعی

بسمه تعالی

شماره:.....
تاریخ:.....
پیوست:.....

سند شرح خدمات تامین و پشتیبانی سرویس ارسال پیامک

۱- مقدمه

گسترده‌گی مأموریت‌ها و تکالیف این وزارتخانه در ارائه ۴۹ خدمت مصوب از سوی سازمان اداری و استخدامی کشور، همچنین ارتقای کارآمدی و بهبود اثربخشی نقش حاکمیتی در راستای خدمت‌رسانی به اقشار و گروه‌های مردمی و کسب و کارهای مختلف، مستلزم اطلاع‌رسانی مؤثر و مستمر در این زمینه می‌باشد. با توجه به مراتب فوق این دستگاه در نظر دارد از سرویس ارسال پیامک که امروزه به عنوان یکی از متداول‌ترین شیوه‌های حوزه اطلاع‌رسانی است بهره‌گیرد. لذا برای تسهیل این امر در نظر است «تامین و پشتیبانی سرویس ارسال پیامک» برای مدیریت ارسال پیامک‌های سامانه‌های تخصصی و عمومی، راه‌اندازی گردد.

۲- اهداف اصلی سامانه

- ارایه پنل پیامکی با امکان اتصال به اپراتورهای تلفن همراه بر اساس پروتکل‌های رایج
- ایجاد ارتباط پایدار و با کیفیت بالای وب سرویس‌ها با اپراتورهای تلفن همراه کشور
- امکان اتصال پنل واسط به سامانه‌های تخصصی از طریق API
- امکان ارسال پیام از طریق پروتکل Smpp
- امکان برقراری ارتباط امن بین سامانه‌ها و اپراتور تلفن همراه
- نظارت و کنترل بر نحوه ارسال پیامک‌ها
- ارایه گزارش‌های آماری از ارسال پیامک‌ها به تفکیک هر سامانه

۳- نتایج پیاده‌سازی سامانه

- اطلاع‌رسانی به جامعه هدف سامانه‌ها در بستر امن
- مدیریت پیام‌های ارسال شده
- اخذ گزارش‌های مدیریتی

۴- ذینفعان

- کاربران متقاضی سامانه‌های دستگاه
- کاربران ستادی استفاده‌کننده از سامانه‌ها
- کاربران مرکز فناوری اطلاعات، ارتباطات امنیت فضای مجازی
- جامعه هدف سامانه‌های تخصصی وزارت تعاون کار و رفاه اجتماعی



جمهوری اسلامی ایران وزارت تعاون، کار و رفاه اجتماعی

بسمه تعالی

شماره:
تاریخ:
پیوست:

۵- واژه نامه

دستگاه: وزارت تعاون، کار و رفاه اجتماعی

جامعه هدف: گروه ها و اقشار مردمی، کاربران ستاد و مرکز فناوری اطلاعات وزارتخانه که به نحوی از سامانه های وزارت متبوع استفاده می نمایند.

سامانه: محصولی است که می تواند متشکل از سخت افزار و نرم افزار، در راستای موضوع و هدف خواسته شده باشد
وب سرویس: نوعی رابط برنامه نویسی است که بر بستر وب پیاده سازی می شود که با استفاده از پروتکل های استاندارد مانند http توابع و مکانیزم های مختلفی را در اختیار ما قرار می دهد تا بتوانیم تبادل اطلاعات در سیستم های مختلف را انجام دهیم.

Otp: رمز یکبار مصرف

پروتکل SMPP: پروتکل استاندارد صنعتی است که به منظور ارائه یک رابط ارتباطی داده انعطاف پذیر برای

انتقال داده های پیام کوتاه بین پیام کوتاه خارجی و مسیریابی و مرکز پیام طراحی شده است.

ترافیک ترانزیت: اگر منبع تولید ترافیک در اپراتوری غیر از اپراتور دریافت کننده ارتباط باشد و به منظور برقراری ارتباط مذکور از کاربر/خدمت برقرارکننده ارتباط به کاربر/خدمت/سرور دریافت کننده ارتباط، مسیردهی به گونه ای صورت پذیرد که ترافیک انتقالی میان متقاضی و دریافت کننده علاوه بر اپراتورهای مبدا و مقصد، از اپراتور میانی دیگری نیز عبور نماید، به ترافیک ایجاد شده در اپراتور میانی، عنوان ترافیک ترانزیتی اطلاق می شود.
پیامک انبوه: به کلیه خدماتی اطلاق می شود که در آن یک پیام به تعداد زیادی از مشترکین تلفن همراه ارسال شود.

پیامک فارسی: به پیامی اطلاق می گردد که فیلد (DCS (Data Coding Scheme آن عدد ۸ باشد. هر پیامک فارسی ۷۰ حرف و هر پیامک غیرفارسی ۱۶۰ حرف غیر خاص در نظر گرفته می شود. در غیر اینصورت پیامک غیرفارسی محسوب می گردد.

۶- قوانین کسب و کار

- مصوبات کمیسیون سازمان تنظیم مقررات رادیویی (مصوبه جلسه شماره ۱۳۳ مورخ ۱۳۹۰/۱۱/۲۵) با موضوع ارسال پیامک های انبوه و سرویس ها و خدمات ارزش افزوده.

۷- شناخت حوزه مسئله

در راستای شرح وظایف کلی سازمان که سیاستگذاری و برنامه ریزی راهبردی در حوزه های مختلف اجتماعی و رفاهی است، سامانه های عمومی و تخصصی به منظور خدمت رسانی به ذینفعان سازمانی راه اندازی شد و از آنجا که بسیاری از خدماتی که از طریق سامانه های مذکور ارائه می شود مستلزم اطلاع رسانی به ایشان است لذا بر همین



جمهوری اسلامی ایران

وزارت تعاون، کار و رفاه اجتماعی

بسمه تعالی

شماره:.....

تاریخ:.....

پیوست:.....

اساس و به منظور مدیریت یکپارچه پیام های ارسالی، مقرر شد پنل پیامکی برای اجرایی نمودن اهداف فوق الذکر راه اندازی گردد.

۸- کاربران و بازیگران (نقش ها)

- ادمین سامانه : ایجاد حساب کاربری، ایجاد دسترسی کاربران سامانه، امکان تعریف سرشماره ، ارسال پیامک تکی و انبوه ، دریافت گزارش ، امکان درج تیکت، تخصیص شارژ بولی برای سامانه، مشاهده میزان شارژ هر سر شماره، مشاهده پیامک های ارسالی
- ادمین سطح دوم سامانه : ارسال پیامک، امکان دریافت گزارش ، مشاهده میزان شارژ سر شماره مربوطه، مشاهده پیامک های ارسالی
- شرکتهای پیمانکار سامانه های عمومی و تخصصی که باید از طریق API به پنل متصل شوند

۹- اجزای اصلی سامانه

اجزای اصلی سامانه را بخش هایی مانند مدیریت دسترسی، گزارشات، تعاملات خارجی با سایر سامانه ها و بخش های تخصصی سامانه ها (زیر سامانه ها) تشکیل می دهند.

۹-۱- مدیریت و کنترل دسترسی سامانه

مدیر سامانه وظیفه مدیریت تمامی دسترسی های لازم به قابلیتها و داده های موجود در سامانه را بر عهده دارد و وظایف او در سامانه به شرح ذیل می باشد:

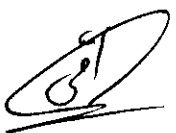
- امکان تعریف ادمین سامانه در چند لایه و چند سطح: سطح اول ادمین فنی و اصلی، سطح دوم ادمین محتوایی و بهره بردار و سطح سوم (با توجه به نوع پروژه و در صورت لزوم تعریف خواهد شد)
- ادمین اصلی و مدیریت فنی سامانه بایستی بتواند تمام دسترسی های لازم برای سایر ادمین ها و سایر کاربران را بر اساس موارد زیر تعریف کند
- امکان افزودن، ویرایش اطلاعات و حذف کاربران
- امکان تغییر رمز کاربران
- امکان ایجاد، ویرایش و حذف گروههای کاربری
- امکان افزودن، ویرایش و حذف کاربران در گروههای کاربری
- امکان تعریف دسترسی به داده ها
- امکان تعریف دسترسی به گزارشات مدیریتی
- امکان مدیریت گروهها به صورت سلسله مراتبی
- امکان دسترسی به داده ها برای گروههای کاربری



- تمامی امکانات سامانه، قابلیت های آن و اجزای سامانه و... توسط ادمین اصلی مدیریت شود و امکان ایجاد دسترسی برای کاربران مورد نظر بر اساس نقش های آنان برای ادمین وجود داشته باشد.
- قابلیت مشاهده لیست تمامی کاربران به همراه مشخصات کاربران: نمایش کد ملی و پست ستادی (برای کاربران ستادی) و شماره همراه و وضعیت آنلاین بودن و گزینه مشاهده جزئیات (جهت نمایش لاگ ها و تاریخ های اتصال به سامانه و نمایش کل فعالیت ها)
- قابلیت مشاهده لیست کلیه کاربران سامانه به همراه سطوح دسترسی مورد نیاز نسبت به اجرای اصلی سامانه (گزارشات، تعاملات خارجی، بخش های تخصصی و زیر سامانه ها) بیان شود.
- طراحی گزارشات و داشبورد مدیریتی
- عناوین گزارشات فهرستی (گزارشاتی که بصورت لیست تهیه میشود) و گزارشات آماری مورد نیاز در سامانه، بیان شود و نمونه گزارشات به پیوست ضمیمه گردد.
- همچنین تولید گزارش ساز پویا به عنوان یکی از الزامات کیفیت نرم افزار در توسعه سامانه ها در پیوست شرح خدمات وجود دارد.

امکان مدیریت حساب های کاربری:

- امکان اتصال به درگاه ارسال پیامک اپراتور تلفن همراه
- امکان تعریف حساب کاربری برای هر کدام از سامانه ها با استفاده از توکن
- امکان تعریف نقش کاربران
- ارایه گزارشات و داشبورد مدیریتی
- امکان تعریف سرشماره ها و اختصاص آن به هر حساب کاربری
- امکان غیر فعال سازی ارسال پیامک از طریق هر یک از سامانه ها در لحظه
- ارسال و دریافت پیام های کوتاه سرویس های قابل ارائه توسط وزارتخانه
- اتصال به مرکز SMS شبکه اپراتور تلفن همراه با حداکثر سرعت ارسال 2000 پیامک در ثانیه از طریق پروتکل ارتباطی مورد توافق طرفین
- قابلیت غیرفعالسازی یا تغییر حسابهای کاربری بلااستفاده به صورت خودکار از طریق انجام تنظیمات در پنل مدیریتی
- قابلیت فعال و غیرفعال سازی ماژولهای غیرضروری سامانه
- مدیریت سامانه های متصل در زمینه تعداد استفاده مجاز از پیامک ها
- مدیریت درخواست های Web API
- تعریف لیست آی پی های مجاز
- امکان مدیریت توکن ها
- قابلیت تهیه بانک اطلاعاتی از مشخصات کاربران
- مدیریت تراکنش های مالی (افزایش اعتبار/تمدید پنل)
- امکان تعریف تعرفه هر پیامک و محاسبه مجموع تراکنش ها بر اساس آن





جمهوری اسلامی ایران

وزارت تعاون، کار و رفاه اجتماعی

بسمه تعالی

شماره:
تاریخ:
پیوست:

- ارسال پیامک هشدار کاهش موجودی حساب سازمان
- تعریف قالب پیامک احراز هویت

امکان مدیریت ارسال ها:

- ارائه گزارشات مدیریتی در فرمت های متداول در حوزه کارکردی و غیر کارکردی با قابلیت فیلتر و مطابق نظر دستگاه
- پشتیبانی از انواع مدل های ارسال پیام کوتاه (تکی، گروهی، ارسال از طریق فایل، پیامک انبوه، از طریق دفترچه تلفن، ارسال نظیر به نظیر، ارسال پویا، ارسال با کد پیگیری، ارسال مناسبتی و ...)
- امکان ارسال پیامک به صورت هوشمند و مکان محور
- امکان ارسال چند باره پیام در بازه های زمانی (روزانه، هفتگی، ماهانه و سالانه) امکان تعریف امکانات دفترچه تلفن، الگوی پیامک، قالب پویا، فیلدهای سفارشی و مناسبت های تقویمی)
- امکان آرشیو نمودن کلیه پیام های ارسالی و دریافتی
- امکان ارسال پیامک در تاریخ و زمان از پیش تعیین شده به صورت دوره ای و تدریجی
- امکان ارسال پیامک انبوه
- امکان ارسال وب هوک
- امکان ارسال پیام به صورت otp
- امکان مدیریت صف ها و صندوق ارسال پیام برای ادمین با امکان فیلتر کردن بر اساس (اکانت/گیرنده/فرستنده/نوع ارسال/وضعیت/تاریخ)
- امکان جستجوی پیشرفته در صندوق و صف ارسال براساس (گیرنده پیام/وضعیت ارسال/وضعیت تحویل گیرندگان/تاریخ و زمان شروع ارسال/تاریخ و زمان پایان ارسال/متن پیام/نوع نقش)
- امکان گزارش گیری از صندوق ارسال سازمان با متن و بدون متن بر اساس (تاریخ/وضعیت پیامک/اپراتور/خط/بخش پیامک/شماره گیرنده/تاریخ و ساعت/متن پیامک/تگ ارسال/شناسه ارسال)
- امکان مدیریت صندوق دریافت و اخذ گزارش های مورد نیاز از آن
- امکان گزارش گیری از شماره های لغو شده و درخواست های لغو با کد ۱۱
- امکان مانیتورینگ اپراتور و گزارش بر اساس (تاریخ/نام اپراتور/خط اختصاصی/وضعیت پیامک)
- امکان گزارش گیری از لیست پرداخت های سازمان بر اساس (تاریخ/وضعیت پرداخت/نوع پرداخت)
- گزارش های آماری ارسال به تفکیک (سال و ماه / وضعیت/ اپراتور/شماره خط) به همراه گزارش نموداری و جدول با امکان خروجی اکسل و PDF
- گزارش آماری وضعیت پیام های ارسالی به همراه گزارش نموداری و جدول با امکان خروجی اکسل و PDF
- گزارش آماری ارسال به تفکیک اپراتور ها به همراه گزارش نموداری و جدول با امکان خروجی اکسل و PDF





جمهوری اسلامی ایران

وزارت تعاون، کار و رفاه اجتماعی

بسمه تعالی

شماره:
تاریخ:
پیوست:

- گزارش آماری جامع به تفکیک اپراتور و وضعیت ها به همراه گزارش نموداری و جدول با امکان خروجی اکسل و PDF

• امکانات اپراتوری:

- در اختیار قراردادن شماره های ذیل :

• ۰۹۲۰۰۰۰۱۱۱۱

• ۰۹۲۰۰۰۰۲۲۲۲

• ۰۹۲۰۰۰۰۱۱۲۲

• ۰۹۲۰۰۰۰۱۱۳۳

• ۰۹۲۰۰۰۰۶۳۶۹

• ۰۹۲۰۰۰۰۶۴۶۹

• ۰۹۲۰۰۰۰۱۱۴۴

- اعمال ماسک "Vezarat.kar" روی شماره ۰۹۲۰۰۰۰۱۱۴۴ و انجام امور مربوط به راهیابی آن در تمام اپراتورها

- ارسال تا سقف ۱۶۰ میلیون پیامک در طول مدت قرارداد (در صورت کاهش یا افزایش تعداد پیامک، برای آن تعداد، هزینه محاسبه خواهد شد).

- ارسال پیامک های ترانزیتی

- ارسال پیامک های otp و Bulk

شرایط پرداخت مبلغ قرارداد به شرکت:

- ۱- ارسال گزارش سه ماهه از پیامک های ارسال شده همچنین ارائه رسید تحویل به مشتری که با فرمول زیر محاسبه و پرداخت می شود:

"تعداد پیامک ارسال شده موفق * مبلغ تعرفه هر پیامک"

- ۲- نحوه محاسبه قیمت کل قرارداد برای بارگذاری در سامانه:

تعداد پیامک * مبلغ هر پیامک

امکانات فنی و امنیتی:

- امکان ایمن سازی سرویس و سرور سامانه
- قابلیت گسترش، سفارشی سازی و ارتقاء براساس نیازهای دستگاه
- عدم نیاز به نصب برنامه های جانبی بر روی کلاینت ها



جمهوری اسلامی ایران

وزارت تعاون، کار و رفاه اجتماعی

بسمه تعالی

شماره:.....

تاریخ:.....

پیوست:.....

- امکان استفاده از مکانیزم احراز هویت دو عامله برای دسترسی به سامانه مدیریت انتقال امن اطلاعات
- سازگاری و عدم تداخل با قواعد دیوار آتش و با امکان اعمال سیاستهای استاندارد امنیتی
- قابلیت استفاده از پروتکل‌های به روز امنیتی برای دسترسی به سرویس مورد نظر و اطمینان از حفاظت کافی
- کلیدهای رمزنگاری
- سازگاری سامانه ارائه شده با ضد بدافزارها
- امکان تنظیم رمز عبور وب سرویس
- تجهیز سامانه به صورت پیش فرض به حداقل یک ضد بدافزار مورد تایید دستگاه
- پشتیبانی از الگوریتم های رمزنگاری رایج و ایمن
- قابلیت مقابله / مقاومت در برابر Script injection SQL injection
- سامانه تولید شده معماری Service Oriented و Clean را پشتیبانی نماید.
- بستر ارتباطی اینترنت، MPLS، over ip
- بستر نرم افزاری ویندوز، لینوکس
- فراهم سازی عملیات به روزرسانی (Update) برای تمامی قابلیت‌های نیازمند به روزرسانی
- رفع عیوب عملکردی

۹-۲- مدیریت تعاملات الکترونیکی خارجی (وب سرویس ها)

- ارائه وب سرویس با استاندارد Rest و Soap به سامانه های دیگر
- قابلیت اتصال به اپراتورهای مختلف براساس پروتکل های رایج





جمهوری اسلامی ایران وزارت تعاون، کار و رفاه اجتماعی

بسمه تعالی

شماره:

تاریخ:

پیوست:

۹-۳- توضیح فرایند مورد انتظار در سامانه (به همراه درج فلوچارت فرایندهای مربوطه)

- درخواست واحد متقاضی جهت استفاده از سرویس مدیریت پیامکی
- بررسی و تایید درخواست متقاضی
- ایجاد اکانت کاربری در سامانه و اختصاص سرشماره به آن
- ایجاد دسترسی و تحویل نام کاربری و رمز عبور به کاربر واحد متقاضی
- ارسال پیامک
- اخذ گزارش های مربوط به ارسال

۹-۴- توضیح پنل های تخصصی

این سامانه دارای پنل تخصصی می باشد.
از طریق این پنل پیامک های سامانه های عمومی و تخصصی ارسال شده، سازماندهی گشته و گزارشات مدیریتی دریافت می گردد.

۹-۵- توضیح نحوه ورود به سامانه (احراز هویت)

نحوه ورود به سامانه بر طبق استانداردهای چک لیست الزامات فنی، کیفی و امنیتی سامانه هاست که به پیوست آمده است.

همچنین در صورت نیاز باید سامانه قابلیت این را داشته باشد که به پنجره واحد وزارتخانه (SSO وزارتخانه) و یا همچنین SSO سازمان فناوری اطلاعات متصل بشود.

(الزامات احراز هویت که در پیوست چک لیست الزامات فنی، کیفی و امنیتی سامانه های تخصصی آمده است، مطالعه شود و با توجه به آن اگر ملاحظه خاص دیگری وجود دارد مطرح شود)

۱۰- مشخصات فنی سامانه

بر اساس ضمیمه چک لیست الزامات و استانداردهای فنی، کیفی و امنیتی توسعه سامانه ها (بند استاندارد و الزامات تکنولوژی)

۱۱- نیازمندیهای غیر کارکردی سامانه

اطلاعات مربوط به نیازمندیهای غیر کارکردی سامانه به شرح ذیل می باشد:

- تعداد پیش بینی کل کاربران سامانه 20.000.000 کاربر

- تعداد پیش بینی کاربرانی که بصورت همزمان از سامانه استفاده می نمایند 2000TPS

۱۱

تهران - خیابان آزادی - نبش بهبودی - وزارت تعاون، کار و رفاه اجتماعی - کدپستی: ۴۵۷۹۹۴۸۶۱
Website : www.mcls.gov.ir Email : info@mcls.gov.ir





جمهوری اسلامی ایران
وزارت تعاون، کار و رفاه اجتماعی

بسمه تعالی

شماره:
تاریخ:
پیوست:

۱۲- پشتیبانی، آموزش و راهنما

پیمانکار موظف خواهد بود پس از توسعه سامانه، بمدت شش ماه ضمانت سامانه تولید شده را بعهدده داشته و از آن به صورت رایگان پشتیبانی کند.

- شرکت موظف به آموزش کامل نحوه بهره برداری از سیستم اعم از پنل های تخصصی و پنل ادمین و سایر اجزای مهم سیستم به کارفرماست.

سایر شرایط مد نظر:

- دارا بودن سامانه تیکتینگ برای ارتباط با پشتیبان سامانه
- ارائه قابلیت پایش مستمر لاگ سرور سامانه و ارسال آن به سامانه مدیریت
- نحوه پشتیبان گیری از سامانه به صورت روزانه می باشد.
- از این سامانه پشتیبانی تخصصی مورد انتظار است به صورتی که نحوه پشتیبانی باید (۲۴ ساعته) باشد
- این سامانه نیاز به پاسخگویی به متقاضیان و ذیتفعان به صورت (برخط و آنلاین/ تلفنی) دارد و ساعات پاسخگویی باید (۲۴ ساعته) باشد.
- شرکت موظف به معرفی یک نفر نماینده تام الاختیار برای پاسخگویی و انجام امور فی مابین است به صورتی که شماره تلفن همراه ایشان در اختیار کارشناسان مرتبط این وزارتخانه قرار گیرد و همیشه در دسترس و پاسخگو باشند.

۱۳- زمانبندی جهت توسعه سامانه

- زمان لازم جهت توسعه سامانه، حداکثر یک ماه از شروع پروژه خواهد بود.





جمهوری اسلامی ایران

وزارت تعاون، کار و رفاه اجتماعی

بسمه تعالی

۱۴- جدول مشخصات درخواست کننده و مستندهای لازم

جدول زیر به همراه لیست مستنداتی که ضمیمه فرم می شود تکمیل گردد.

جدول مشخصات درخواست کننده و مستندهای لازم

نام واحد درخواست کننده سامانه: مرکز فناوری اطلاعات و امنیت فضای مجازی	تاریخ درخواست: ۱۴۰۵/۰۳/۰۳
نام نماینده تام الاختیار: امیر علی امی	شماره تماس: ۶۴۴۹۲۶۵۲
نام رابط با فناوری اطلاعات: عاطفه تیموری	شماره تماس: ۶۴۴۹۲۷۱۲
لیست مستندات مرتبط: ۱- ۲- ۳- ۰ ۰ ۰ (فرم ها، نمونه گزارشات، گردش کار و موارد قانونی که باید ضمیمه فرم سند شرح خدمات سامانه گردد)	





جمهوری اسلامی ایران

وزارت تعاون، کار و رفاه اجتماعی

بسمه تعالی

شماره:

تاریخ:

پیوست:

پیوست شماره ۱: ضمیمه لیست الزامات تخصصی پیمانکاران و توسعه سامانه ها

الزامات پیمانکاران شرکت کننده در سامانه ستاد دولت:

۱. شرکت باید به دقت شرح خدمات را مطالعه کند و تمام موارد خواسته شده از جمله مدارک تخصصی را بارگذاری نماید وگرنه به درخواست آنها ترتیب اثر داده نخواهد شد.
۲. تیم پروژه معرفی شده از سوی پیمانکار می بایست کامل و توانمند بوده و شرکت موظف است مشخصات اعضا و افراد درگیر پروژه را بنا بر نقش های آنها در تیم و سطح تخصص ایشان و میزان زمانگذاری در پروژه و در نهایت نفر/ساعت را طبق جدول استاندارد نظام صنفی مشخص کند و در سامانه ستاد دولت بارگذاری نماید.
۳. شرکت دارای تخصص ویژه در زمینه تهیه و پشتیبانی نرم افزار و سامانه تخصصی مورد نظر باشد (اگر سوابق مشابه دارد در سامانه ستاد دولت بارگذاری نماید)
۴. شرکت دارای گواهینامه رتبه بندی و احراز صلاحیت معتبر شرکت های انفورماتیکی معتبر از سازمان برنامه و بودجه کشور در زمینه تولید نرم افزار سفارش مشتری، فناوری اطلاعات و ارتباطات با رتبه ۱ تا ۴
۵. دارای مجوز های لازم از سازمان تنظیم مقررات و ارتباطات رادیویی مبنی بر ارسال پیامک
۶. دارای گواهینامه عضویت معتبر از سازمان نظام صنفی رایانه ای
۷. شرکت موظف است حداقل ۲۴ ساعت پیش از هرگونه به روز رسانی سیستم ها، مراتب را به اطلاع این دستگاه برساند.
۸. شرکت متعهد است که کلیه استانداردهای لازم و رایج را جهت ارسال و دریافت پیام از طریق پروتکل SMPP و یا هر پروتکل دیگر مورد توافق از جمله استاندارد لازم برای ارسال پیامهای فارسی و غیرفارسی، پیامهای طولانی (Long SMS) و غیره را در شبکه خود فراهم نماید.
۹. شرکت موظف بر نظارت بر کیفیت، کمیت، حجم پیامهای ارسالی و دریافتی از سمت وزارتخانه می باشد.
۱۰. اپراتور تلفن همراه موظف است گزارش کتبی تعداد پیامکهای ارسالی شماره های موضوع این قرارداد را بصورت تفکیک شده و ماهیانه در اختیار وزارتخانه قرار دهد.
۱۱. دارای گواهی امنیتی افتا (دریافت مجوز افتا ریاست جمهوری پس از خاتمه تولید محصول طی بازه زمانی سه ماهه الزامی می باشد)





جمهوری اسلامی ایران
وزارت تعاون، کار و رفاه اجتماعی

بسمه تعالی

شماره:.....

تاریخ:.....

پیوست:.....

۱۲. دارای گواهی حسن سوابق همکاری با سایر دستگاه ها

۱۳. شرکت پیمانکار موظف به پشتیبانی ۲۴ ساعته از سرویس ارسال پیامک بوده و در صورت بروز هر گونه

اختلال در ارسال پیامک موظف است مشکل پیش آمده را در اسرع وقت مرتفع نماید.

سایر الزامات جهت توسعه سامانه :

۱۴. مالکیت مادی و معنوی سامانه یا نرم افزار و مالکیت بر کل فرآورده های پروژه (اعم از کد منبع، برنامه های

اجرایی، سورس، دیتا و اطلاعات کامل بارگذاری شده از لحظه شروع پروژه تا زمان مورد نیاز، برند، مالکیت

مادی و معنوی، پایگاه ها و مدل های داده ای، مدل های فرآیندی و مستندات و مدارک فنی) منحصراً متعلق

به کارفرما و در اختیار وزارتخانه است. در پایان پروژه در صورت رضایت ناظر پروژه، تائیدیه انجام کار اعطا

خواهد شد.

۱۵. شرکت موظف به آموزش کامل نحوه بهره برداری از سامانه اعم از پنل های تخصصی و پنل ادمین و سایر

اجزای مهم سامانه به کارفرماست.

۱۶. شرکت ملزم به مشارکت در اصلاح و تکمیل فرآیندهای پیشنهادی و توسعه کسب و کار در صورت درخواست

کارفرما است

۱۷. شرکت موظف به آموزش تکنولوژیهای استفاده شده در تهیه سامانه به همکاران مرکز فناوری اطلاعات

وزارت متبوع می باشد.

۱۸. ارائه گزارش آخرین تغییرات در سامانه به صورت دوره ای به ناظر پروژه

۱۹. رعایت چک لیست الزامات و استانداردهای فنی، کیفی و امنیتی

۲۰. ارائه گواهینامه معتبر تست نفوذ سامانه

۲۱. تمامی پایگاه داده های ساخته شده می بایست توضیحات کامل مرتبط به خود و همچنین ارتباطات خود

باسایر جدول ها را داشته باشد و نیز هر column می بایست متناسب با استفاده ای که میشود comment

گذاری گردد.

۲۲. شرکت موظف است از آخرین ورژن پایدار فریم ورک ها یا سورس ها و برنامه های مورد نیاز استفاده نماید.





جمهوری اسلامی ایران

وزارت تعاون، کار و رفاه اجتماعی

بسمه تعالی

شماره:.....

تاریخ:.....

پیوست:.....

۲۳. ساختار MVC بایست در کل پروژه رعایت شود.

۲۴. قابلیت ابر پذیری سامانه ها: زیرساخت یکپارچه ابری مجموعه ای از فناوری ها، سرویس ها و راهکارهایی

است که برای ایجاد یک محیط ابری و متمرکز استفاده می گردد. این زیرساخت شامل سرورهای ابری، شبکه

های ابری، ذخیره سازی ابری و مدیریت محیط ابری است.

۲۵. افزودن موارد یا انجام تغییراتی که هر ساله در قالب شاخص های پایش خدمات الکترونیکی دولت از دبیرخانه

شورای عالی فناوری اطلاعات ابلاغ می گردد.





جمهوری اسلامی ایران
وزارت تعاون، کار و رفاه اجتماعی

بسمه تعالی

شماره:.....
تاریخ:.....
پیوست:.....

پیوست شماره ۲: چک لیست الزامات و استانداردهای فنی، کیفی و امنیتی سامانه های تخصصی

الزامات و استانداردهای کیفیت			
توضیحات	عنوان	ردیف	نیمک
➤ الزامات تست های کیفیت (quality)			
	موفقیت در تست در دسترس بودن صفحه از طریق وب سایت https://www.wakav.ir (بالاتر از ۹۹ درصد باشد)	۱	
	موفقیت در تست سرعت از طریق وب سایت https://www.wakav.ir (میانگین درصد بزرگتر از ۹۰ باشد)	۲	
	موفقیت تست راندمان از طریق وب سایت https://www.wakav.ir (میانگین درصد بزرگتر از ۹۰ باشد)	۳	
	انجام تست های کیفیت مانند: Fuctional testing, Non-functional testing, interface testing (UI Testing), performance testing, unit test, component testing, load testing, stress testing, alpha test, beta testing, volum testing,	۴	
➤ استاندارد و الزامات تکنولوژی :			
	سامانه به درگاه SSO دولت و وزارتخانه متصل باشد (در صورت درخواست کارفرما)	۵	
	استفاده از داده های دیتابیس از طریق API باشد	۶	
➤ احراز هویت (در صورت عدم اتصال به SSO سازمان)			
	دریافت صرفاً کدملی و شماره تماس جهت ثبت نام	۷	
	دریافت کدملی، شماره تماس و پست سازمانی (برای کاربران سازمانی و متناسب با نوع بیزینس کسب و کار) جهت ثبت نام	۸	
	استفاده از وب سرویس شاهکار	۹	
	استفاده از وب سرویس ثبت احوال	۱۰	
	ثبت نام و ورود از طریق رمز یکبار مصرف (تایید کد پیامک شده)	۱۱	



 جمهوری اسلامی ایران
 وزارت تعاون، کار و رفاه اجتماعی

شماره:.....
 تاریخ:.....
 پیوست:.....

الزامات و استانداردهای کیفیت			
ردیف	عنوان	توضیحات	نیمک
۱۲	قراردادن زمانشمار جهت وارد کردن رمز یکبار مصرف (حداکثر دو دقیقه)		
۱۳	قابلیت تعریف گذرواژه ثابت از سمت کاربر وجود داشته باشد. (برای تعریف نام کاربری، به طور پیش فرض کد ملی فرد به عنوان نام کاربری انتخاب می شود)		
۱۴	قابلیت بازیابی رمز عبور در صورت فراموشی رمز عبور		
۱۵	ورود صرفاً از طریق رمز ثابت باشد (نام کاربری هم باید کد ملی فرد باشد)		
۱۶	مکانسیم تعیین هویت، در نتیجه تلاش های ناموفق به منظور تعیین هویت، جزئیات مربوط به ناموفق بودن تصدیق را به فراخوان گزارش دهد.		
۱۷	تعداد دفعات تلاش های ناموفق به منظور تعیین هویت (در زمان ورود به سیستم و یا هر یک از نواحی امن) دارای محدودیت باشد		
۱۸	کد امنیتی جهت ورود وجود داشته باشد و این کد شامل صرفاً عدد باشد. برای سامانه های خیلی حساس نیز ترکیبی از عدد و حرف (غیرحساس به حروف بزرگ و کوچک) باشد.		
۱۹	هنگام ورود گذرواژه امکان مشاهده توسط کاربر وجود داشته باشد (در صورت تمایل خود کاربر)		
➤ پشتیبانی و راهنما			
۲۰	وجود بخش راهنمای pdf		
۲۱	دارای سیستم تیکتینگ		
۲۲	وجود شماره تماس جهت پاسخگویی به سوالات (پشتیبانی تلفنی)		
➤ وب سرویس ها			
۲۳	استفاده از سرویس پیام رسان های ایرانی جهت اطلاع رسانی به کاربران) علاوه بر سرویس ارسال پیامک)		
۲۴	پیاده سازی وب سرویس هایی از خدمات سامانه (بر اساس نظر کارشناس وزارتخانه)		
۲۵	استفاده از وب سرویس های موجود در وزارتخانه جهت الکترونیکی نمودن کامل فرآیند دریافت خدمت		
➤ الزامات و قابلیت های ضروری			





جمهوری اسلامی ایران

وزارت تعاون، کار و رفاه اجتماعی

بسمه تعالی

شماره:
تاریخ:
پیوست:

الزامات و استانداردهای کیفیت			
نیک	ردیف	عنوان	توضیحات
	۲۶	امکان گزارش گیری های مدیریتی به صورت پویا و از تمام اقلام اطلاعاتی موجود در سامانه (گزارش ساز پویا)	
	۲۷	پنل مدیریتی، گزارشی با تعریف سطح دسترسی داشته باشد. ستاد و استان و شهرستان به صورت داینامیک	
	۲۸	دارای سیستم تیکتینگ (برای تمامی کاربران اعم از ستادی و عادی)	
	۲۹	امکان لاگ گیری از تمامی کاربران در لایه اینترفیس (بر اساس بند مدیریت لاگ گیری در شرح خدمات)	
	۳۰	امکان مانیتورینگ کاربران (تعداد کل کاربران، تعداد کل کاربران آنلاین، نمایش نموداری کل کاربران متصل بر اساس روز، ساعت، سال، امکان drill down شدن و نمایش فعالیت هر کاربر به طور مجزا)	
	۳۱	دارای کنسول مدیریتی باشد.	
	۳۲	امکان اطلاع رسانی در صفحه اصلی (جهت اطلاع رسانی ها و اخبار ضروری در مواقع لزوم)	
	۳۳	قابلیت واکنش گرایی (responsive بودن) به ابزار های مختلف مانند موبایل، تبلت و کامپیوتر رومیزی (Cross Browser بودن) به معنای سازگاری صفحات سامانه با انواع مرورگرها. (Findable بودن) وب سایت ساختار مناسبی داشته باشد و اطلاعات به راحتی در دسترس باشد. (Contrast ratio بودن) تفاوت بین روشنایی بین متن و پس زمینه باید حداقل 4.5 برابر باشد.	
➤ مدیریت نشست ها			
	۳۴	طول زمانی اعتبار نشست ها دارای محدودیت باشد.	
	۳۵	نشست هایی که کاربر آن غیرفعال است، توسط سیستم شناسایی شود و پس از حداکثر ۳۰ دقیقه بسته شوند.	
	۳۶	کاربر سامانه بتواند فرمان خاتمه نشست (LOG OUT) را صادر کند.	
	۳۷	نشست ها به صورت تصادفی ساخته شود.	
➤ الزامات و استانداردهای زیرساخت			
	۳۸	توپولوژی زیرساخت مشخص باشد. به صورت داکيومنت شده	





الزامات و استانداردهای کیفیت			
توضیحات	عنوان	ردیف	تیک

الزامات و استانداردهای امنیت

این پیوست، جزء لاینفک قرارداد بوده و پیمانکار موظف به اجرای مفاد و شرایط آن است.

بخش اول - شرایط کلی

۱. مجوزها و تاییدیه‌ها
 - در صورت استفاده از محصولات آماده، محصول باید تاییدیه امنیتی از مرکز مدیریت راهبردی افتا داشته باشد.
 - در صورت توسعه محصول، شرکت پیمانکار باید دارای مجوز رسمی از مرکز مدیریت راهبردی افتا باشد.
۲. وابستگی به محصولات خارجی
 - محصول باید حداقل وابستگی به محصولات خارجی داشته باشد و شرکت پیمانکار باید تضمین تداوم عملکرد محصول را ارائه دهد.
۳. تامین اجزای مستقل محصول
 - تامین بخش‌ها، اجزا یا مولفه‌های مستقل نرم‌افزاری محصول مانند سیستم‌عامل، وب سرور، پایگاه داده و برنامه‌های شخص ثالث (مانند فریم‌ورک‌ها و کتابخانه‌ها) باید توسط شرکت پیمانکار انجام شود.
۴. مسئولیت امنیت محصول
 - شرکت پیمانکار مسئول تامین امنیت محصول شامل به‌روزرسانی‌ها، وصله‌های امنیتی و مقاوم‌سازی براساس شرایط تعریف شده توسط وزارت خانه است.





الزامات و استانداردهای کیفیت			
توضیحات	عنوان	رابط	بیک
۵. فرآیندهای نظارت و ممیزی امنیتی			
• معاونت امنیت وزارت خانه متولی فرآیندهای نظارت و ممیزی امنیتی محصول بوده و شرکت پیمانکار نیز باید نسبت به اقدامات اصلاحی و ارائه گزارش متعهد باشد.			
۶. کانال ارتباطی امن			
• یک کانال ارتباطی امن بین وزارت خانه و شرکت پیمانکار برای اطلاع رسانی در خصوص کشف و رفع آسیب پذیری ها ایجاد شود. اگر وزارت خانه به آسیب پذیری ای پی برد، باید در سریع ترین زمان ممکن از طریق این کانال به شرکت پیمانکار اطلاع دهد.			
۷. دسترسی ها			
• براساس الزامات وزارت خانه های ناظر، امکان ارائه هیچ گونه دسترسی راه دور وجود ندارد			
۸. تغییر اطلاعات پیش فرض			
• تغییر نام کاربری و کلمه عبور پیش فرض تمامی سرویس های مرتبط با محصول از جمله پایگاه داده باید قبل از انتشار انجام شود.			
۹. محیط عملیاتی و تست			
• محیط عملیاتی و محیط تست باید از یکدیگر مجزا باشد. هرگونه توسعه و یا استفاده از ابزارهای توسعه روی سرورهای عملیاتی مجاز نیست.			
۱۰. استفاده از نسخه های به روز			
• پیمانکار موظف است از آخرین نسخه های پایدار اجزای مستقل مانند وب سرورها و پایگاه داده ها استفاده کرده و آخرین وصله های امنیتی را نصب نماید.			
۱۱. معماری استقرار محصول			
• پیمانکار باید معماری استقرار محصول (نحوه قرار گرفتن محصول در محیط عملیاتی) و اطلاعات دیگر مانند پلتفرم ها، تکنولوژی ها و وابستگی های محصول به نرم افزارها و کتابخانه های شخص ثالث را ارائه دهد.			





الزامات و استانداردهای کیفیت			
ردیف	عنوان	توضیحات	بیک
۱۲.	محدودسازی پورت‌ها و سرویس‌ها		
	• پیمانکار با نظارت وزارت خانه باید پس از استقرار محصول محدودسازی پورت‌ها و سرویس‌ها را انجام دهد.		
۱۳.	مقاوم‌سازی پیش از عملیاتی شدن		
	• محصول باید پس از استقرار و قبل از عملیاتی شدن، بر اساس چک‌لیست‌های امنیتی مقاوم‌سازی شود و وزارت خانه باید بر این فرآیند نظارت داشته باشد. این مقاوم‌سازی شامل اپلیکیشن، اجزا و سیستم عامل می باشد.		
۱۴.	زمانبندی وصله‌های امنیتی		
	• وزارت خانه باید کشف آسیب‌پذیری‌ها را به پیمانکار اعلام کند و پیمانکار موظف است ظرف ۷۲ ساعت راهکارهای برای جلوگیری از تهدیدات را ارائه دهد و وصله‌های امنیتی لازم را فراهم کند.		
۱۵.	نرم‌افزارهای پورتال سازمانی و مدیریت محتوا		
	• پیمانکار باید مکانیزم‌های تشخیص و جلوگیری از حملات Deface را برای نرم‌افزارهای پورتال سازمانی و سیستم مدیریت محتوا ارائه دهد.		
۱۶.	سیستم عامل ها و اجزا نرم افزاری		
	• سیستم عامل های مجاز و ماژول های نرم افزارای مجاز توسط وزارت خانه تعیین و ابلاغ می گردد. پیمانکار جهت استفاده از اجزا نرم افزاری ملزم به استعلام کتبی می باشد. در صورتی که بنا به دلایل امنیتی یک جزء نرم افزاری قابلیت استفاده نداشته باشد پیمانکار موظف به تغییر و جایگزینی آن است.		





جمهوری اسلامی ایران
وزارت تعاون، کار و رفاه اجتماعی

بسمه تعالی

شماره:.....
تاریخ:.....
پیوست:.....

الزامات و استانداردهای کیفیت			
نیک	ردیف	عنوان	توضیحات
بخش دوم : الزامات مربوط به توسعه امن نرم افزار			
در تمامی سامانه ها و نرم افزارها موارد زیر باید رعایت شود.			
		• پیاده سازی مکانیزم تصدیق هویت کاربران به شیوه ای امن و قابل اعتماد. • سامانه می بایست امکان پشتیبانی از احراز هویت دوعاملی را داشته باشد. • کنترل ورودی های کاربر در سمت سرور برای جلوگیری از حملاتی مانند دور زدن کنترل های سمت کاربر (مثل جاوااسکریپت). • مکانیزم های جلوگیری از حملات به صفحات ورود مانند حملات Brute Force و Credential Stuffing. • سیاست های قوی برای انتخاب نام کاربری و کلمه عبور براساس استانداردهای امنیتی. • تغییر پیام های خطای پیش فرض در صورت ورود ناموفق و عدم افشای اطلاعات حساس به کاربر. • تغییر صفحات خطای پیش فرض اپلیکیشن و وب سرور • کنترل دقیق حقوق دسترسی کاربران در تمامی قسمت های سامانه و اپلیکیشن. برای این موضوع نیاز به مکانیزم های کنترل سطح دسترسی در تمامی قسمت ها و ویژگی های سامانه می باشد. • مکانیزم جلوگیری از حرکت در دایرکتوری ها (Directory Traversal) و پیاده سازی راهکارهای جلوگیری در سطح نرم افزار و وب سرور • کنترل دسترسی به منابع سیستم براساس اصل حداقل مجوز. • اجرای سرویس های نرم افزار با کمترین مجوز لازم به منظور کاهش ریسک های امنیتی. • حفاظت از نشست های کاربری و شناسه های آنها در طول انتقال اطلاعات روی شبکه با استفاده از پروتکل های امن (مانند HTTPS) و مکانیزم های امنیتی مانند SSL/TLS. • استفاده از پروتکل امن https • مدیریت نشست ها و انتخاب شناسه های امن برای نشست ها (Session Management). • عدم ذخیره سازی اطلاعات حساس در نشست های پایدار و قابل دسترسی. • کنترل ورودی ها در سمت سرور و عدم اعتماد به کنترل های سمت کاربر به تنهایی.	





الزامات و استانداردهای کیفیت			
توضیحات	عنوان	ردیف	تیک
• پیاده‌سازی مکانیزم‌های امنیتی برای جلوگیری از حملات اجرای کد جاوااسکریپت روی کاربر (XSS). • مکانیزم‌های جلوگیری از حملات تزریق کد به پایگاه داده (SQL Injection). • جلوگیری از آسیب‌پذیری سرریز بافر و دیگر آسیب‌پذیری‌های مرتبط با حافظه. • جلوگیری از اجرای کد از راه دور روی سیستم‌عامل (RCE). • مکانیزم‌های جلوگیری از جعل درخواست‌ها (CSRF) با پیاده‌سازی CSRF Tokens و یا سایر اقدامات فنی دیگر • مدیریت صحیح خطاها و استثناءها به منظور عدم افشای اطلاعات حساس. • رمزنگاری داده‌های حساس قبل از ارسال بر روی شبکه در تمامی سرویس‌های مورد استفاده اپلیکیشن • استفاده از مقادیر تصادفی امن و غیرقابل پیش‌بینی در مولدهای تصادفی. • عدم ذخیره‌سازی داده‌های حساس در سمت کاربر و مرورگر. • رویدادنگاری دقیق و مفهومی از وقایع امنیتی در سطح برنامه‌های کاربردی و سرویس‌ها. • جلوگیری از استفاده از متدهای ناامن HTTP و اطمینان از استفاده از متدهای امن مانند POST به جای GET برای درخواست‌های حساس. • غیرفعال‌سازی امکان فهرست کردن فایل‌ها بر روی وب سرور. • جلوگیری از آسیب‌پذیری‌های مربوط به SSRF (Server-Side Request Forgery). • جلوگیری از آسیب‌پذیری‌های LFI و RFI (Local/Remote File Inclusion). • پیاده‌سازی مکانیزم‌های مناسب برای تنظیمات CORS به منظور جلوگیری از سوءاستفاده. • جلوگیری از آسیب‌پذیری‌های Open Redirect. • جلوگیری از آسیب‌پذیری SSTI (Server-Side Template Injection). • جلوگیری از حملات افزایش سطح دسترسی در سطح برنامه‌های کاربردی. • بررسی نشست کاربر و کنترل سطح دسترسی در تمامی ماژول‌ها و صفحات سامانه • استفاده از مکانیزم CAPTCHA در صفحه ورود سامانه و در فراخوانی عملکردهای حساس • استفاده از مکانیزم‌های Rate Limit در فراخوانی توابع و مسیرهای سامانه • ذخیره‌سازی فایل‌های آپلود شده در مسیری خارج از دایرکتوری سرور			





الزامات و استانداردهای کیفیت			
توضیحات	عنوان	ردیف	تیک

- بررسی فایل‌های آپلود شده و محتوای آنها
- بررسی حجم فایل‌های آپلود شده توسط مکانیزم‌های سمت سرور
- مدیریت Exception ها و خطاهای سرور و اپلیکیشن و شخصی‌سازی خطاها
- استفاده از هدرهای امنیتی و تنظیم مناسب آنها در پاسخ‌های سرور
- عدم ذخیره‌سازی گذرواژه و اطلاعات حساس در پایگاه داده بصورت متن واضح
- عدم ذخیره‌سازی اطلاعات احراز هویت سرور بصورت متن واضح در فایل‌های تنظیمات
- جلوگیری از افشای مسیر کامل فایل‌ها در پیام‌های خطا.
- پیاده‌سازی فرآیند و برنامه دقیق برای به‌روزرسانی و نصب وصله‌های امنیتی برای سیستم‌عامل، وب سرور، مازول‌ها و کتابخانه‌هایی که در تولید و توسعه نرم‌افزار استفاده می‌شوند.

بخش سوم : الزامات مربوط به امنیت سورس و توسعه

- استفاده از استاندارد معتبر و بروز از قبیل SSDLC
- بررسی سورس با استفاده از چک لیست های امنیتی مانند OWASP
- استفاده از ابزارهای بررسی امنیتی سورس برنامه (مانند SAST و DAST) در طول فرآیند توسعه
- برای شناسایی زودهنگام آسیب‌پذیری‌ها و ارایه گزارش و تفسیر قبل از انتشار
- رمزنگاری اطلاعات حساس در پایگاه داده‌ها به همراه مدیریت کلیدهای رمزنگاری
- پیمانکار موظف به تحویل سورس برنامه های توسعه داده شده براساس نیاز وزارت خانه است
- پیمانکار موظف به تحویل سند معماری و شناخت می باشد

بخش چهارم : الزامات به‌روزرسانی و برطرف‌سازی آسیب‌پذیری‌ها

- شرکت پیمانکار می‌بایست لیست کاملی از تمامی نرم‌افزارها، کتابخانه‌ها، فریم‌ورک‌ها و ... که در توسعه نرم‌افزار مورد استفاده قرار گرفته است را به وزارت خانه ارائه دهد.
- شرکت پیمانکار می‌بایست بصورت ماهیانه و مرتب نسخه نرم‌افزارها، کتابخانه‌ها، فریم‌ورک‌ها و ... که در توسعه نرم‌افزار و اپلیکیشن مورد استفاده قرار گرفته است را به‌روزرسانی نماید.





الزامات و استانداردهای کیفیت			
توضیحات	عنوان	ردیف	تیک
- در صورت اعلام و یا کشف آسیب پذیری توسط تیم امنیت وزارت خانه از نرم افزارها، کتابخانه ها، فریم ورک ها و ماژول های مورد استفاده برای توسعه اپلیکیشن و سامانه پیمانکار، شرکت پیمانکار موظف است در سریعترین زمان ممکن نسبت به به روز رسانی و رفع آسیب پذیری ها اقدام نماید. - شرکت پیمانکار موظف به اجرای سیاست های امنیتی اعلامی کارفرما برای بر طرف سازی و رفع آسیب پذیری ها می باشد. - شرکت پیمانکار موظف به اجرای سیاست های امنیتی اعلامی کارفرما برای به روز رسانی امنیتی و اعمال وصله های امنیتی و رفع آسیب پذیری ها می باشد. - شرکت پیمانکار موظف است قبل از اعمال وصله های امنیتی و تغییر در سامانه ابتدا در محیط تست و توسعه شرایط را کامل بررسی نموده و در صورت عدم وجود مشکل، در محیط عملیاتی تغییرات را اعمال نماید یا نسخه نرم افزار را به روز نماید. - شرکت پیمانکار قبل از ارائه نسخه نهایی نرم افزار و سامانه و منتشر نمودن در محیط عملیاتی وزارت خانه می بایست تاییدیه از تیم امنیت دریافت نماید. این تاییدیه منوط به انجام فرآیند ارزیابی امنیتی و تست نفوذ توسط تیم امنیتی وزارت خانه می باشد. - شرکت پیمانکار می بایست سازگار مناسب برای نسخه گذاری و مدیریت تغییرات سامانه را داشته باشد و در صورت نیاز به تیم امنیت وزارت خانه ارائه نماید. - شرکت پیمانکار باید محیط تست و توسعه را از محیط عملیاتی بصورت کامل جداسازی نماید.			

بخش پنجم: الزامات ثبت و جمع آوری رخدادهای

- شرکت پیمانکار موظف است سامانه های موضوع قرارداد را به شکلی توسعه دهد که امکان ارائه لاگ رخدادهای سامانه به مرکز عملیات امنیت را دارا باشد.
- شرکت پیمانکار به منظور ارسال رخدادهای سامانه می بایست حریم شخصی و صیانت از اطلاعات محرمانه را در نظر داشته باشد و نسبت به محوسازی و مخفی نمودن اطلاعات حساس و محرمانه درون رخدادهای اقدامات لازم را صورت دهد.
- سامانه می بایست قابلیت ثبت تمامی فعالیت های کاربران را دارا بوده و در صورت درخواست مقامات قضایی، امکان ارائه آن وجود داشته باشد





جمهوری اسلامی ایران

وزارت تعاون، کار و رفاه اجتماعی

بسمه تعالی

شماره:
تاریخ:
پیوست:

الزامات و استانداردهای کیفیت

توضیحات	عنوان	ردیف	تیک
---------	-------	------	-----

بخش ششم: الزامات مربوط به ارتباطات سامانه

- در تمامی سیستم‌های اطلاعاتی، کانال‌های انتقال داده باید به دقت شناسائی، و بستر ارتباطی (شبکه) آنها نیز مشخص شده، و پس از آنها مخاطرات آنها ارزیابی شود. این اطلاعات و ارزیابی باید توسط شرکت توسعه‌دهنده و واحد امنیت وزارت خانه صورت پذیرد.
- کانال‌های ارتباطی مانند ارتباط کاربر به سامانه، سامانه با پایگاه داده، سامانه با سرویس‌ها و API‌ها و ... می‌بایست بصورت امن و رمزنگاری شده با استفاده از پروتکل‌های قوی صورت پذیرد.
- در پیاده‌سازی پروتکل‌ها و ارتباطات امن می‌بایست به‌روش پیاده‌سازی مدنظر قرار گیرد.
- حتماً می‌بایست از پروتکل https و TLS برای ارتباطات وب استفاده گردد. همچنین برای پیاده‌سازی این پروتکل‌ها به‌روش امنیتی می‌بایست در نظر گرفته شود تا از آسیب‌پذیری‌های احتمالی این پروتکل‌ها جلوگیری به عمل آید.

