موضوع : پیوست فنی ، شرح خدمات ، ابزارهای مورد استفاده و فازهای پیاده سازی سامانه آرشیوالکترونیک اسناد

شرح قید حفظ امنیت و محرمانگی :

احراز هویت : احراز هویت فرایند شناسایی منحصر به فرد نرم‌افزار است.

اعطای حق دسترسی : اعطای حق دسترسی فرایندی است که در آن، منابع و عملیاتی که کاربران احراز هویت شده اجازه دسترسی به آنها را دارند، مدیریت می‌شود. منابع شامل فایل‌ها، اسناد ، اطلاعات کاربران و .. است.

حسابرسی : حسابرسی و رویدادنگاری، کلید عدم انکار است. عدم انکار بدین معناست که یک کاربر نمی‌تواند انجام کاری یا شروع .یک تراکنش را در سیستم انکار کند ، زیرا تمامی فعالیت های کاربر در سامانه ثبت شده است.

محرمانگی : محرمانگی که به آن «حریم خصوصی» هم گفته می شود ، فرایند اطمینان حاصل کردن از این است که داده‌ها محرمانه و خصوصی می‌مانند و توسط کاربرانی که مجوز ندارند یا استراق سمع‌کنندگانی که به ترافیک شبکه نظارت می‌کنند، دیده نیز ابزار دیگری است ACLنمی‌شوند. رمزگذاری اغلب برای رسیدن به این هدف به کار گرفته می‌شود. لیست کنترل دسترسی که با همین هدف استفاده می‌شود.

صحت : صحت تضمین‌کننده این است که داده‌ها از هر گونه تغییر عمدی یا تصادفی محافظت می‌شوند. «صحت» داده از اهمیت بسیار زیادی به خصوص وقتی روی شبکه مبادله می‌شود برخوردار است. «صحت» داده هنگام نقل و انتقال عمدتا توسط روش‌های Hashing یا کدهای احراز هویت پیام فراهم می‌شوند.

دسترس‌پذیری : در دایره امنیت ، «دسترس‌پذیری» یعنی اینکه سیستم برای کاربران معتبر در دسترس باشد. هدف بسیاری از مهاجمان با حملات از نوع انکار خدمت این است که برنامه کاربردی سقوط کند تا مطمئن شوند که کاربران دیگر نمی‌توانند به برنامه دسترسی داشته باشند.

شرح خدمات در محدوده موضوع:

موضوع قرارداد عبارت است از تدوین ، طراحی و پیاده سازی سامانه ارشیو الکترونیکی اسناد با امکانات موارد مندرج زیر:

۱. قبل از پیاده سازی UI ، باید طراحی صفحات و منوهای مختلف در قالب فایل psd ، برای کارفرما ارسال شود . در صورت عدم تایید کارفرما اصلاحات انجام گیرد . پس از تایید طراحی صفحات جهت پیاده سازی UI اقدام شود. نحوه ی پیاده سازی UI به صورت المان در داخل برنامه با کنترلر ها تعریف شده باشد و قابلیت addو remove داشته باشد.

۲. برنامه نویسی پروژه به صورت Clean Code انجام گیرد : کد تمیز مجموعه ای اصول کدنویسی است که باعث می شود دیگران بتوانند کد را بخوانند و آن را توسعه دهند.سادگی،خوانایی و قابل فهم بودن،نام گذاری مناسب،مدیریت آرگومان ها،عدم کامنت گذاری،کاهش وابستگی،تست پذیری و کاهش حجم توابع از ویژگی های اصلی یک کد تمیز است .

۳. طراحی منو صفحات مختلف ، صفحه لاگین، صفحه اصلی ، منوی اصلی به صورت navigation ، صفحه ی مدیریت کاربران ، صفحه ی ایجاد سند ، ثبت ، ویرایش و جستجو سند ، صفحه ی گزارشات لاگ کاربران و لاگ اسناد. صفحه ی گزارش گیری بر اساس فیلتر های مختلف ، صفحه ی بک آپ گیری، صفحه کارتابل مدیر (مدیریت کاربران) و فرم ساز پویا

٤. استفاده از Authentication برای تایید هویت افراد و Authorization برای کنترل دسترسی کاربران به بخش های مختلف سایت .

٥. ثبت نام کاربر، لاگین براساس نوع کاربر: امکان ثبت نام کاربر با درج اطلاعات هویتی شخص ، و تایید مدیر سامانه و تعریف سطوح دسترسی متنوع برای ایشان وجود دارد. بعد از ورود کاربر جلسه استارت میخورد و درصورت عدم فعالیت ایشان برای مدت زمانی مشخص جلسه منقضی میشود و با نمایش پیغام مربوطه کاربر باید مجددا لاگین کند.

٦. ایجاد سیستم امنیت و سطوح دسترسی برای مدیر، کارشناس و کاربر (این سه مدل به صورت پیش فرض در سامانه وجود دارند) مدیر سایت دسترسی کنترل کامل دارد ، کارشناس سایت دسترسی ساخت و ویرایش و مشاهده دارد اما دسترسی دیلیت ندارد . کاربر فقط دسترسی مشاهده دارد. مدیر سامانه قابلیت افزودن مدل جدید(مدل ها محدودیت تعداد ندارند) و ویرایش و تخصیص سطوح مختلف دسترسی و تخصیص مجوزهای مشاهده، ویرایش، دانلود، آپلود ، تعریف کاربر ، ایجاد سند ، انتساب سند و ... بصورت checkbox به هر کاربر را دارد .

٧. فرم سازی پویا :

برای ثبت هر سند در سامانه نیاز هست کارشناس یا کاربر مشخصات سند را در فرم مخصوص ثبت سند در سامانه وارد کند. فیلدهای این فرم ، ممکن است تغییر کند و در زمان بهره برداری از سامانه ممکن است به هر دلیل متوجه شویم که این فرم نیاز به چند فیلد یا لیبل جدید دارد، ادمین سامانه باید بتواند از طریق سامانه و نه کدنویسی، این فرم ها را تغییر دهد و چند فیلد یا لیبل را تغییر دهد ، پاک کند ، بیافزاید و یا ویرایش کند.

٨. ایجاد سند ، ساخت پوشه های تو در تو ، قفسه بندی(پوشه بندی) اسناد، ارتباط با اسناد و تعریف زیرمجموعه برای هر سند، تعریف سطح بندی اسناد به صورت درختی تا حداکثر ده سطح .

علاوه بر افراد، هر سند ثبت شده در سامانه قابل دسته بندی به صورت درختی می باشد. برای مثال در دسته اسناد پرسنلی چند دسته سند برای بازنشستگان وظیفه بگیران، شاغلین خواهیم داشت. تعریف اسناد ، نام گذاری سطوح ، .. به صورت پیش فرض نباشد و هر نوع نام گذاری توسط کاربری که دسترسی دارد قابل انجام باشد .نام گذاری پوشه ها و اسناد با هر پیشوند و پسوندی امکان پذیر باشد. استاندارد regex . یک سری فیلد به صورت دیفالت برای هر سند وجود داشته باشد اما مدیر بتواند فیلد های دلخواه خود را برای هر سند خاص اضافه کند و نوع دیتای آن فیلد نیز دلخواه مدیر باشد . یک قسمت attachment نیز در نظر گرفته شود تا امکان ثبت تصاویر ویا هر فایل با هر پسوند به اسناد(پیوست و پانوشت و جزئیات) وجود داشته باشد.

٩. امکان نسبت دادن یک سند به یک کاربر برای پیگیری یا تکمیل بهتر است در داشبورد مدیریت وجود داشته باشد. یعنی مدیر بتواند یک سند را انتخاب و فرضا lable گذاری کند که باید توسط کدام کارشناس تکمیل شود وکارشناس هم در پروفایل خود به سند دسترسی داشته باشد . در کارتابل کاربر روی پیغام ها یک نوتیفیکیشن در زمانی که سند ارجاع داده می شود ظاهر شود (مثلا با عنوان شما یک پیغام جدید دارید ، در زمان باز شدن صفحه ی پیغام ها به نمایش در آید که سند جدید به شما ارجاع داده شد .)

۱۰. تعریف زمان اعتبار برای اسناد: بعد از دسترسی به هر سند تایمر استارت خواهد خورد و بعد از انقضای زمان مشخص امکان مشاهده و یا دریافت اسناد برای کاربر عادی وجود ندارد. (دسترسی به تمامی اسناد حتی منقضی شده ها برای مدیر وجود داشته باشد) (تایمر توسط ایجاد کننده سند قابل تنظیم باشد)

۱۱. امکان ثبت تصاویر با پسوند رایج تصویری اعم از : tiff،bmp، png, jpg, ,gif, psd فایل با پسوند به اسناد , pdf , multi excel ,.docx doc ,vsd ,pptقابلیت ثبت خواهند داشت. امکان ذخیره سازی مجموعه ای از اسناد به صورت pdf ، tiff امکان پذیر باشد .(انتخاب این مجموعه برای کاربر امکان پذیر باشد مثلا یک پوشه یا دو پوشه از اسناد یا دو عدد سند متفاوت در پوشه های جدا)

۱۲. امکان جست و جو بر اساس هرنوع اطلاعات و فیلدهای موجود در سند : فرم جستجو با اعمال فیلترهای متنوع مانند کدسند یا کدکلاسه سند،کد محدوده ، نام پوشه ، تاریخ ثبت ، نوع سند (این موارد ممکن است تغییر کند در حین پیاده سازی)وجود خواهد داشت.

۱۳. امکان ثبت ورود و خروج اسناد از محل قفسه ها به صورت دیجیتالی : تمام عملیاتی که کاربر روی سند انجام میدهد، از جمله ورود و خروج و ویرایش و ثبت اسنادو حذف سند ، درج خواهد شد و با لاگ گیری قابل مشاهده خواهد بود. هر زمان که سند ساخته میشود در دیتابیس نیز فیلد های مربوط ساخته شود و هر زمان که سند پاک میشود از دیتابیس نیز پاک شود.

۱۴. امکان جلوگیری از تکرار و وجود سیستم خودکنترلی:

سامانه زمان ثبت سند جدید بصورت خودکار جداول را جستجو میکند و اگر سند با آن مشخصات قبلا ثبت شده باشد امکان ثبت مجدد را ندهد و پیغام خطای مربطه را برای اطلاع کاربر نمایش دهدو از کاربر سوال کند که اطلاعات تکراری است آیا دوباره می خواهید که ذخیره شود؟ اگر فایل attach شده نیز تکراری باشد ارور دهد و از کاربر بپرسد که این فایل تکراری است آیا دوباره می خواهید که ذخیره شود ؟

در زمان ثبت سند جدید بعد از جستجو جداول لیستی حاوی اسناد مشابه نمایش دهد تا کاربر اگر تمایل داشت سند جدید را به آن سند مرتبط کد یا در پوشه ی اسناد مشابه قرار دهد (تمامی فیلد های اسناد بررسی و در صورت مطابقت در این قسمت نمایش داده شوند).

۱۵. امکان شخصی سازی بر اساس نیاز سازمان :

وجود چند تم رنگی که داشبورد شخصی سازی شود و تم قابل انتخاب باشد.

۱۶. امکان اتصال به سامانه دیگر سازمان از طریق ایجاد و پیاده سازی وب سرویس :

از آنجا که کل سامانه موضوع این قرارداد بصورت Web API پیاده سازی می شود، امکان برقراری ارتباط با سامانه دیگر از طریق وب سرویس وجود دارد، که این امر مستلزم همکاری کارفرما برای تبادل اطلاعات و پروتکلهای مورد نیاز سامانه دیگر ایشان می باشد. ارتباط این سامانه با سامانه دیگر سازمان بصورت دوطرفه به منظور ارسال و دریافت اطلاعات انجام خواهد شد که جزئیات اطلاعات مورد نیاز برای تبادل توسط کارفرما ابلاغ خواهد شد.

۱۷. سیستم مدیریت کاربران و ایجاد کارتابل مدیر ارشد: این امکان در داشبود مدیریت وجود خواهد داشت با توجه به مندرجات بند۴ ، که ثبت سابقه فعالیت هر کاربر در کارتابل مدیر قابل دسترس باشد . در کارتابل مدیر کنار هر مدل (کاربر) یک لینک باعنوان سابقه فعالیت وجود داشته باشد و با کلیک روی آن یک فرم یا صفحه بسته به سلیقه برنامه نویس باز شود و فعالیت کاربر را از ابتدا تا آن تاریخ نمایش دهد. بنابراین چرخه حیات یا سابقه فعالیت برای کاربران حتی مدیر ارشد و تمامی اسناد وجود داشته باشد.

۱۸. تولید گزارش های پویا: امکان تولید گزارش ها بصورت نمودار دو بعدی, دایره ای، آماری و سایر انواع نمودار های گرافیکی و همچنین خروجی اکسل از روند ثبت اسناد با اعمال فیلترهای متنوع از جمله بازه زمانی ثبت یا تولید سند، نوع اسناد ، کارشناس یا کاربر ثبت کننده ، حجم سند، شهر یا استان مربوط به سند، کلاسه و... وجود داشته باشد.
(نوع فیلترها توسط مدیر قابل حذف یا اضافه کردن باشد)

۱۹. امکان مشاهده لاگ هر سند و گردش کار هر سند و گردش کار هر کاربر:
برای تمام عملیات کاربر و همچنین تمام عملیاتی که روی هر سند از زمان ورود اجرا می شود می توان لاگ دریافت کرد. در کنار هر سند یک لینک تحت عنوان چرخه حیات سند وجود داشته باشد و با کلیک روی آن workflow مربوط به سند باز شود . (نمودار نمایش داده شده اتصال یک سری نقطه (وضعیت) است که با ایستادن موس روی هر نقطه اطلاعات مربوط به نمایش در می آید. مثلا :
نقطه ی اول (create by admin , date :1399/10/10)
نقطه ی دوم (edit by admin , date : 1399/10/20)
با کلیک روی نقطه ها سند همان وضعیت ، هر چند که حال تغییر کرده باشد باز شود.

۲۰. ذخیره سازی فایلها روی هارد و درج آدرس در پایگاه داده (بصورت file stream):
امکانی برای کاربر سامانه فراهم میشود تا از آن طریق فایلها را در مکان مشخصی از هارد ذخیره کند که آدرس آن فولدر بصورت خودکار در جداول ذخیره خواهد شد . می توان این عملیات را از طریق sql server و file group انجام داد.
فولدری را از هارد به پایگاه داده معرفی میکنیم به محض حذف فایل از آن فولدر به صورت اتومات ادرس هم از جداول حذف شود و به محض تشکیل یک فایل آدرس نیز در جداول ذخیره شود .

۲۱. امکان بازخوانی اطلاعات و تهیه بک آپ :
بکاپ گیری با استفاده از تعریف یک تسک DBA در سامانه قابل پیاده سازی است.
فرض بر این است که سازمانی که این نرم افزار را خریداری کرده است از دیتابیس هایش بک آپ نمیگیرد و باید بکاپ گیری از طریق این نرم افزار انجام شود و دارای زمان بندی باشد و قابل انتخاب و تغییر توسط ادمین نرم افزار باشد{فیلد های قابل تغییر : (بک آپ گیری روزانه ، هفتگی ، ماهانه)، تایم بک آپ گیری (ساعت و زمان) ، مکان بک آپ گیری} مشابه نرم افزار veeambackup. (سامانه به صورت اتوماتیک باید بک آپ بگیرد)
کنترل صحت تولید پشتیبان:هر بک آپ ۳ حالت داشته باشد (در حال انجام ، موفق ، ناموفق) اگر ناموفق است علت را هم نمایش دهد مثلا به دلیل پر بودن لوکیشن انتخاب شده برای ذخیره ی بک اپ و حجم ناکافی.

۲۲. مدیریت سوابق گردش اسناد : یعنی اگر مدیر تمایل داشت سند به وضعیت قبلی خود برگردد یا به وضعیت دو ماه قبل خود برگردد این امکان وجود داشته باشد . اما سوابق اسناد همچنان ذخیره بماند مگر اینکه مدیر عمدا نیازی به سوابق نداشته باشد و به صورت دستی سوابق را پاک کند.

ابزارهای مورد استفاده در این پروژه

موضوع پروژه به صورت WebAPI پیاده سازی شود و بکند و فرانت کاملا مستقل از هم باشند .

- استفاده از پروتکل Restful برای پیاده سازی وب سرویس
- بهره مندی identity server برای وب سرور و IIS 10
- تکنولوژی پیاده سازی بک اند سامانه ASP.Net Core 3.1 خواهد بود.
- زبان مورد استفاده در فرانت اند HTML5 – Css3 - Javascript خواهد بود.
- استفاده از **Entity Framework** و **Object Relational Mapping** (**ORM**) برای ارتباط سامانه با پایگاه داده و امکان Manipulate یا دستکاری داده بدون اتصال مستقیم به پایگاه داده بمنظور وجود سهولت در تغییر احتمالی پایگاه داده در آینده و پشتیبانی از انواع پایگاه داده و همچنین امکان اجرا روی پلتفرم های مختلف مانند لینوکس.
- نوع دیتابیس پیاده سازی سامانه :SQL SERVER ۲۰۱۷
- معماری پیاده سازی سامانه : استفاده از معماری میکروسرویس برای کل سامانه هست.
- استفاده از : متدهای جستجوی سریع و realtime در پایگاه داده مثل shrink , index .... جهت جلوگیری از افت کارایی و سرعت بعد از حجیم شدن رکوردهای پایگاه داده

فازهای پیاده سازی:

پیاده سازی نرم افزار به صورت VCS (version control system) باشد و محدود به زبان برنامه‌نویسی خاص و همچنین ویرایشگر کد خاصی نباشد.
موضوع قرارداد در ۵ فاز طبق متدولوژی اسکرام و رویکرد چابک (agile) انجام خواهد شد و در نرم افزار جیرا تمام فازهای پروژه و پیشرفت آن توسط واحد زیرساخت ثبت و توسط فریلنسر قابل مشاهده خواهد بود.
تحویل سورس پروژه باید به صورت مرحله ای انجام گیرد ، هر ۵ روز یکبار سورس جدید باید درسرور گیت شرکت آپلود شود .

فازهای تعریف شده کلی طراحی و پیاده سازی موضوع قرارداد به شرح زیر است:

ردیف	موضوع	توضیحات
فاز اول	طراحی معماری پایگاه داده و طراحی و تحلیل واسط کاربریUI,UX	فلوچارت روند کلی سامانه و نمودار ارتباط موجودیتها ERD سامانه در این مرحله ترسیم و به کارفرما تحویل داده میشود. واسط کاربری و تجربه کاربری طراحی و به منظور اعلام سلیقه و تایید کارفرما به ایشان تحویل میشود.
فاز دوم	پیاده سازی واسط کاربری UI, UX	توسعه و پیاده سازی واسط کاربری و تجربه کاربری تایید شده
فاز سوم	کدنویسی و پیاده سازی backend	طراحی و توسعه تمامی موارد موضوع قرارداد به غیر از وب سرویس
فاز چهارم	پیاده سازی وب سرویس	پیاده سازی وب سرویس برای ارتباط با سامانه دیگر، برقراری ارتباط و تست تبادل اطلاعات
فاز پنجم	استقرار و تست سامانه	تست کارایی (performance) ، تستهای تجمیعی، استقرار نهایی و ارائه نرم افزار به کارفرما

امنیت:

شرح قید حفظ امنیت و محرمانگی : تمامی موارد مربوط به احراز هویت، اعطای حق دسترسی ، حسابرسی و رویدادنگاری ، محرمانگی ، صحت داده در کل نرم افزار تحت وب مذکور لازم الاجراست. لطفا با شرکت تماس بگیرید https://digi-doc.ir تمامی متودولوژی ها برای تست نفوذ وب اپلیکیشن مطابق با OWASP ، در حوزه های زیر بررسی شده و باید پاس گردد :

تزریق، احراز هویت شکسته ، لو رفتن اطلاعات حساس ، کنترل دسترسی شکسته ، عدم پیکر بندی درست امنیت ، استفاده از اجزایی با اسیب پذیری های شناخته شده ، لاگین و پایش ناکافی، XXE، XSS، Insequre deserialization