



بیمه آریان

# دستورالعمل امنیت اطلاعات و فرآیند پیگیری در مدیریت فاوا

شماره سند :  
WI-IT-01/01

شماره صفحه	شماره تجدید نظر	تاریخ	شرح تغییرات
کلیه صفحات	00	۱۳۹۶/۰۶/۲۴	صدور اولیه

تهیه کننده / بازنگری کننده	تایید کنندگان		تصویب کننده / ابلاغ کننده
مدیریت فناوری اطلاعات و ارتباطات	مدیریت تحقیق و توسعه	معاونت توسعه و پشتیبانی	مدیرعامل

این دستورالعمل مهور به مهر آبی "اعتبار دارد" دارای اعتبار است.







# دستورالعمل امنیت اطلاعات و فرآیند پیگیری در مدیریت فاوا

شماره سند: WI-IT-01/02  
تاریخ: ۱۳۹۶/۰۶/۲۴  
پیوست: دارد  
صفحه: ۱ از ۵

## ۱- هدف

هدف از تدوین این دستورالعمل، استاندارد سازی و شفاف سازی تعاملات کلیه پرسنل ستاد و شعب در راستای رعایت امنیت اطلاعات و تشریح موارد و مراحل مرتبط با فرآیند پیگیری درخواست های خود از پرسنل مدیریت فناوری اطلاعات و ارتباطات (فاوا) در شرکت بیمه آرمان می باشد.

## ۲- دامنه کاربرد:

دامنه کاربرد این دستورالعمل، در ستاد و شعب بیمه آرمان در سراسر کشور می باشد.

## ۳- مسئولیت ها:

مسئولیت اجرای این دستورالعمل بر عهده کلیه پرسنل ستاد و شعب شرکت می باشد و مسئولیت نظارت بر حسن اجرای این دستورالعمل بر عهده مدیریت فاوا بیمه آرمان می باشد.

## ۴- مدارک ذیربط:

- ۴-۱- فرم تحویل سیستم به کاربر جدید (به شماره FM-IT-01-01)
- ۴-۲- فرم درخواست نصب نرم افزار (به شماره FM-IT-02-01)
- ۴-۳- فرم کپی اطلاعات (به شماره FM-IT-03-01)
- ۴-۴- فرم درخواست اینترنت (به شماره FM-IT-04-01)
- ۴-۵- فرم درخواست کالا (به شماره FM-IT-05-01)
- ۴-۶- فرم تحویل کارت ریج (به شماره FM-IT-06-01)
- ۴-۷- فرم بررسی تجهیزات (به شماره FM-IT-07-01)
- ۴-۸- فعال سازی دسترسی مازاد یا اعمال محدودیت خاص در نرم افزار اتوماسیون اداری گام (به شماره FM-IT-08-01)
- ۴-۹- فعال سازی دسترسی مازاد یا اعمال محدودیت خاص در نرم افزار فناوران (به شماره FM-IT-09-01)
- ۴-۱۰- فرم جابه جایی سیستم (به شماره FM-IT-10-01)
- ۴-۱۱- فرم دسترسی به پوشه مشترک (به شماره FM-IT-11-01)
- ۴-۱۲- فرم درخواست درج اطلاعات در وب سایت (به شماره FM-IT-12-01)
- ۴-۱۳- راهنمای دسترسی به اینترنت سازمان (به شماره HD-IT-01-01)

## ۵- تعاریف:

ندارد.



# دستورالعمل امنیت اطلاعات و فرآیند پیگیری در مدیریت فاوا

شماره سند: WI-IT-01/02  
تاریخ: ۱۳۹۶/۰۶/۲۴  
پیوست: دارد  
صفحه: ۲ از ۵

## ۶- نحوه اجرا:

در راستای رعایت امنیت اطلاعات و مراحل مرتبط با فرآیند پیگیری درخواست از مدیریت فاوا، در ذیل جزئیات نحوه اجرا ذکر شده است.

ردیف	عنوان	توضیحات
۱	امنیت اطلاعات (تحویل اطلاعات کاربری)	با توجه به لزوم حفظ محرمانگی رمز عبور کلیه پرسنل موظف خواهند بود در اولین ورود به نرم افزارهای سازمانی یا سیستم رایانه خود، رمز عبور آن را تغییر دهند.
۲	امنیت اطلاعات (فراموشی رمز عبور)	در صورت فراموشی رمز عبور یکی از نرم افزارهای سازمانی، کلیه پرسنل ستاد و شعب موظف هستند به صورت مکتوب درخواست خود را از طریق پیام یا نامه اتوماسیون برای مدیریت فاوا ارسال نمایند. همچنین برای نمایندگان شرکت فقط پرسنل امور نمایندگان می توانند درخواست مکتوب جهت دریافت رمز عبور جدید آن نماینده را ارسال کنند.
۳	امنیت اطلاعات (ارسال درخواست مکتوب)	کلیه درخواست های پرسنل ستاد و شعب در مدیریت فاوا، فقط از طریق ارسال درخواست به صورت مکتوب انجام می گردد. بنابراین خواهشمند است قبل از ارسال درخواست به صورت نامه، تکمیل فرم یا پیام مربوطه به این مدیریت، از تماس تلفنی جهت پیگیری درخواست خود پرهیز نمایید.
۴	امنیت اطلاعات (دسترسی)	ایجاد نام کاربری و رمز عبور در نرم افزارهای سازمانی شرکت به صورت پیش فرض دسترسی سمت اشخاص تعیین شده است. مدیریت یا معاونت مافوق هر قسمت می تواند با تکمیل فرم مربوطه و ارسال آن به پیوست نامه درخواست، برای یک پرسنل در صورت نیاز به فعال سازی دسترسی بیشتر یا اعمال محدودیت خاص اقدام نماید.
۵	امنیت اطلاعات (سوء استفاده)	هر یک از پرسنل موظف به حفظ نام کاربری و رمز عبور خود می باشند و نباید در اختیار دیگر همکاران شرکت قرار گیرد. بدیهی است عواقب هرگونه سوء استفاده از نام کاربری و رمز عبور یک نفر، بر عهده ی خود پرسنل می باشد.
۶	امنیت اطلاعات (ورود به سیستم)	کلیه پرسنل موظف خواهند بود منحصراً فقط روی سیستم تحویل گرفته خود، با اطلاعات کاربری خود وارد شوند و نمی توانند از طریق سایر سیستم ها به شبکه داخلی ورود کنند.
۷	امنیت اطلاعات (نصب نرم افزار)	جهت نصب هر گونه نرم افزار غیر سازمانی، کلیه پرسنل شرکت موظف هستند فرم نصب نرم افزار را تکمیل و پس از تایید مدیریت مافوق به مدیریت فاوا به صورت مکتوب ارسال نمایند. بدیهی است عواقب هرگونه سوء استفاده از نرم افزارهای غیر سازمانی بر عهده ی کاربر و مدیریت واحد مربوطه خواهد بود.



## دستورالعمل امنیت اطلاعات و فرآیند پیگیری در مدیریت فاوا

شماره سند: WI-IT-01/02

تاریخ: ۱۳۹۶/۰۶/۲۴

پیوست: دارد

صفحه: ۳ از ۵

استفاده از شبکه های اجتماعی بر روی سیستم های شرکت ممنوع است و می بایست کلیه مکاتبات با خارج از شرکت از طریق ایمیل سازمانی (اوتلوک) یا نرم افزار اتوماسیون اداری انجام شود.	امنیت اطلاعات (مکاتبه با خارج از شرکت)	۸
بدون هماهنگی با این مدیریت از اتصال کابل شبکه با نودهای شبکه این سازمان جدا خودداری فرمائید. توجه شود که امکان استفاده برای کاربران به دلیل امنیت اطلاعات غیرفعال است.	امنیت اطلاعات (شبکه)	۹
اتصال به شبکه داخلی این سازمان به معنای داشتن اینترنت نیست. در صورت نیاز به استفاده از اینترنت می بایست فرم درخواست مربوطه توسط کاربر با تایید مدیریت مافوق به مدیریت فاوا به صورت مکتوب ارسال گردد.	امنیت اطلاعات (شبکه)	۱۰
کلید کاربران مجاز برای استفاده از اینترنت در ساختمان میرداماد و ساختمان غرب می بایست روزانه یکبار با اطلاعات کاربری سیستم ویندوز خود به صفحه مرورگر سیستم اعتبار سنجی اینترنت وارد گردند. خواهشمند است جهت توضیحات بیشتر فایل راهنمای دسترسی به اینترنت سازمان مطالعه شود.	امنیت اطلاعات (شبکه)	۱۱
هیچ کاربری امکان استفاده از نرم افزارهای ریموت در داخل شرکت را ندارد و می بایست مدیر مافوق با ذکر دلیل نامه ای خطاب به مدیریت فاوا ارسال کند و مجوز توسط این مدیریت صادر گردد.	امنیت اطلاعات (شبکه)	۱۲
پرسنل شرکت موظف هستند فقط از سایت های مرتبط و مجاز استفاده نمایند و دسترسی به سایت های غیر مرتبط در شبکه داخلی شرکت محدود گردیده است.	امنیت اطلاعات (شبکه)	۱۳
برای هر مدیریت، پوشه مشترکی در شبکه ایجاد شده است که در صورت نیاز به دسترسی پرسنل به آن، می بایست فرم مربوطه تکمیل گردیده و با تایید مدیریت مافوق و تعیین سطح دسترسی پرسنل (خواندن، خواندن و نوشتن یا دسترسی کامل) به مدیریت فاوا به صورت مکتوب ارسال گردد.	امنیت اطلاعات (شبکه)	۱۴
کلید پورت های خروجی سیستم های شرکت به خصوص پورت های اینترنتی، ریموتی، usb و ایمیل، بسته است و در صورت درخواست مکتوب از مدیریت مافوق جهت باز شدن یک پورت، قابل انجام می باشد.	امنیت اطلاعات (شبکه)	۱۵
کلید کاربران در داخل شرکت از طریق پروکسی به اینترنت متصل می شوند و ترافیک استفاده آنها به صورت حجمی مدیریت وسایط های باز شده رهگیری می شوند.	امنیت اطلاعات (شبکه)	۱۶
تمامی کاربران اعم از ستاد، شعب و نمایندگان در صورت استفاده از فیلترشکن نمی توانند با نرم افزارها و سرورهای سازمانی بیمه ارتباط برقرار کنند.	امنیت اطلاعات (شبکه)	۱۷
تمامی شعب فقط از طریق دریافت IP استاتیک از سرویس دهنده اینترنت خود می توانند به ستاد متصل شوند. مدیریت محترم شعبه قبل از تغییر سرویس دهنده	امنیت اطلاعات (شعب)	۱۸



# دستورالعمل امنیت اطلاعات و فرآیند پیگیری در مدیریت فاوا

شماره سند: WI-IT-01/02

تاریخ: ۱۳۹۶/۰۶/۲۴

پیوست: دارد

صفحه: ۴ از ۵

یا جابه جایی شعبه، موظف است IP استاتیک سرویس دهنده جدید اینترنت را به صورت مکتوب به مدیریت فاوا اعلام نماید.		
تمامی نمایندگان و کارگزاران شرکت نمی توانند به صورت مستقیم با این مدیریت در ارتباط باشند و می بایست کلیه درخواست های آنها، فقط از طریق مدیریت شعبه مربوطه یا مدیریت امور نمایندگان به صورت مکتوب ارسال و پیگیری گردد.	امنیت اطلاعات (شعب و امور نمایندگان)	۱۹
تمامی نمایندگان شرکت می بایست حداکثر تا پایان سال ۱۳۹۷، اقدام به دریافت IP استاتیک از سرویس دهنده اینترنت خود نمایند. در غیر اینصورت در سال آینده نمی توانند به نرم افزارهای سازمانی این شرکت متصل شوند.	امنیت اطلاعات (شعب و امور نمایندگان)	۲۰
در سنهاب (درگاه ورود به سامانه های بیمه ی مرکزی) هر کاربر فقط با یک IP می تواند وارد سامانه شود.	امنیت اطلاعات (سنهاب)	۲۱
کلیه کاربران در نرم افزار بیمه گری فناوران موظف هستند که مشکلات سیستمی خود را به مدیریت فنی مربوطه اعلام نمایند تا نسبت به رفع مشکل اقدام شود و در صورت عدم رفع مشکل، درخواست از طرف مدیریت فنی مربوطه به مدیریت فاوا به صورت مکتوب ارسال می گردد.	نرم افزار فناوران (پیگیری درخواست)	۲۲
فعال شدن بیمه گذاران و بیمه شده های غیرفعال و نامعتبر در سیستم، کاربران موظف هستند درخواست خود را به مدیریت فنی بیمه نامه مربوطه ارسال نمایند؛ مدیریت فنی مربوطه در صورت تایید موظف است به صورت مکتوب از طریق نامه یا پیام در اتوماسیون درخواست فعال سازی را به مدیریت فاوا ارسال نماید و مسئولیت آن متوجه مدیریت فنی مربوطه خواهد بود.	نرم افزار فناوران (بیمه گذار غیرفعال)	۲۳
افزودن یک قابلیت جدید در نرم افزار بیمه گری فناوران در حوزه مختلف بیمه می بایست با تایید شورای فنی و معاونت فنی به صورت مکتوب به مدیریت فاوا اعلام گردد.	نرم افزار فناوران (قابلیت جدید)	۲۴
ثبت بیمه گذاران حقوقی فقط توسط مدیریت فناوری اطلاعات با ارسال درخواست مکتوب انجام می شود و منوط به ارسال تمامی مشخصات بیمه گذار حقوقی اعم از شناسه ملی، کد اقتصادی، نوع مالکیت، شماره تلفن ثابت، شماره همراه و ... می باشد. در صورتیکه هر کدام از اطلاعات ناقص باشد امکان ثبت وجود ندارد.	نرم افزار فناوران (بیمه گذار حقوقی)	۲۵
در نرم افزار اتوماسیون اداری گام ارجاعات تمام کاربران (به جز مدیران) در صورتی که به مقام هم پایه یا مافوق خود نباشد بسته است و این دسترسی تنها در صورت تکمیل فرم مربوطه توسط مدیریت مافوق و مدیریت فاوا تغییر می کند.	نرم افزار اتوماسیون اداری (ارجاعات)	۲۶
برای امور دبیرخانه ای و شماره گذاری در شعب فقط و فقط یک پرسنل از طرف مدیریت مافوق به صورت مکتوب به مدیریت فاوا معرفی می گردد.	نرم افزار اتوماسیون اداری (دبیرخانه شعب)	۲۷



## دستورالعمل امنیت اطلاعات و فرآیند پیگیری در مدیریت فاوا

شماره سند: WI-IT-01/02

تاریخ: ۱۳۹۶/۰۶/۲۴

پیوست: دارد

صفحه: ۵ از ۵

۲۸	نرم افزار اتوماسیون اداری (تعریف امضاء)	به دلیل اینکه امضای هر فرد باید منحصر به فرد و ثابت باشد و اعتبار محتوای یک نامه با امضا آشنا و ثابت شخص مسئول معتبر می باشد؛ امکان تعریف امضا در نرم افزار اتوماسیون اداری برای کاربران مسئول بیش از یک بار نیست.
۲۹	جابه جایی سیستم	جابه جایی سیستم ها بدون اطلاع و هماهنگی با این مدیریت امکان پذیر نمی باشد و می بایست فرم جابه جایی توسط مدیریت مافوق پرسنل تکمیل و ارسال گردد. عواقب هرگونه خسارات بدون اطلاعات مدیریت فاوا به عهده پرسنل می باشد.
۳۰	خرابی قطعات	کلیه پرسنل شرکت موظف هستند که در حفظ اموال در اختیار خود، نهایت دقت و مراقبت را داشته باشند و در صورت هرگونه خرابی با تکمیل فرم مربوطه درخواست خود را جهت تعمیر با تعویض به مدیریت فاوا ارسال نمایند.
۳۱	درخواست کالا یا کاتریج	کلیه پرسنل شرکت موظف هستند که جهت دریافت کالا یا تعویض کاتریج فرم مربوطه درخواست را تکمیل کنند و به صورت مکتوب به مدیریت فاوا ارسال نمایند.
۳۲	قرارداد همکاری با پیمانکار	کلیه پیمانکاران در حوزه فناوری اطلاعات و ارتباطات می بایست قبل از عقد قرارداد و ارائه خدمات به این شرکت، در جلسه ای مشترک با مدیریت فاوا نوع خدمت، منابع مورد نیاز، نوع پشتیبانی و سایر بررسی های فنی را انجام دهند. بنابراین خواهشمند است مدیریت یا معاونت محترم مربوطه به اهمیت امنیت اطلاعات و فرآیند کاری عقد قرارداد مرتبط با مدیریت فاوا در این شرکت توجه فرمایند.
۳۳	امنیت اطلاعات (محرمانگی و مالکیت)	کلیه اطلاعات و اسناد بدست آمده در زمان همکاری با شرکت بیمه آرمان محرمانه بوده و متعلق به این شرکت می باشد و پرسنل اجازه دریافت کپی و خارج کردن آنها را ندارند. همچنین پرسنل نباید اطلاعات شخصی خود را بر روی سیستم های سازمانی کپی کنند. فقط در صورتیکه مدیریت مافوق پرسنل شخصی بودن یک داده و شاخه آن را تایید نماید؛ با تکمیل فرم مربوطه و ارسال مکتوب از طرف مدیریت مافوق به مدیریت فاوا، کپی در اختیار پرسنل قرار می گیرد.
۳۴	امنیت اطلاعات (تسویه حساب)	پرسنل شرکت در صورت قطع همکاری و تسویه حساب موظف هستند که اموال و اقلام دریافتی خود را به صورت صحیح و سالم به همراه کلیه اطلاعات رایانه به مدیریت واحد مربوطه تحویل دهند و مدیریت واحد مربوطه موظف است به صورت مکتوب تاییدیه دریافت اطلاعات و اموال پرسنل را به مدیریت فاوا اطلاع دهند. توجه شود که بدون داشتن این نامه، فرم تسویه حساب پرسنل در این مدیریت تایید نمی گردد.