



وزارت بهداشت درمان و آموزش پزشکی
هیات مرکزی گزینش

رازداری و حفاظت اسناد



مدرس : م . پایان [عضو هیات علمی دانشکده فارابی و گروه علمی اجا]

فصل اول: رازداری (حفاظت گفتار)

بخش ۱ - کلیات رازداری و امانت داری

۱- پیش گفتار :

ضعف نفس، پُرحرفی، عقده حقارت، دوستی و رفاقت، احساساتی شدن از عوامل افشای راز هستند، اشخاص پرحرف، برای اشباع برخی کمبودها، از هر دری سخن به میان می‌آورند و یافته‌های خویش را به دیگران انتقال می‌دهند، چنین کاری سبب پرده برداشتن از اسرار آدمی و دربرخی موارد، موجب افشای اسرار اداری می‌گردد.

گفت پیغمبر که هر که سرّ نهفت

زود گردد با مراد خویش جفت

دانه‌ها، چون در زمین پنهان شود

سرّ آن، سرسبزی بستان شود

زر و نقره، گر نبودندی نهان

پرورش کی یافتندی زیر کان

راز مترادف سرّ، آن چه باید در دل نهفته باشد و چیزی که باید پنهان بماند یا به اشخاص مخصوصی گفته شود، اطلاق می‌گردد.

حفظ اسرار را باید از خدا آموخت. خداوند بیش‌تر و پیش‌تر از هر کس، از اعمال، حالات، رفتار، عیوب و گناهان بندگان با خبر است، اما حلم، بردباری، پرده‌پوشی و رازداری او بیشتر از همه است.

هرکس از نظر اخلاقی و عملی، نگرش و خصوصیات دارد که دیگران آن را نمی‌بینند و از آن اطلاعی ندارند، این ویژگی‌ها، رازهای شخصی‌انسان محسوب می‌شود، حال سخن در این است که آیا انسان می‌تواند رازهایش را برای دیگران بازگو کند؟ انسان عاقل سینه خود را صندوقچه اسرارش قرار می‌دهد و از طریق رازداری، خود را از پیامدهای ناگوار افشای اسرار، مصون می‌دارد. به همان مقدار که راز داری شخصی در موفقیت انسان، نقش دارد، افشای آن نیز موجب ناکامی انسان در رسیدن به هدف‌ها می‌شود و گاهی موجب پشیمانی انسان شده و غم و اندوه را با خود به میان می‌آورد.

نیروهای هر سازمان در زندگی خصوصی، خواه ناخواه اسراری دارند که بایستی در نگه داری آن کوشا باشد. برخی از این اسرار شخصی و برخی مربوط به سیستم اداری و اطلاعاتی است که به موجب شرح وظایف شغلی به آن دسترسی پیدا می‌کنند. و این اطلاعات نزد آنها امانت است، لزوم مکتوم ماندن این اسرار به جهت حساسیت و امکان فراوان سوء استفاده عوامل اطلاعاتی سرویس‌های بیگانه و دشمنان از آنها، از نظر اخلاقی، شرعی، اداری و قوانین ابلاغی، پسندیده و جایز نیست.

سخندان پرورده پیر کهن

بیاندیشد آنگه بگوید سخن

(سعدی)

۲ - حکایت :

غلامی طبق سرپوشیده‌ای بر سر داشت و خاموش و بی‌صدا در راهی می‌رفت. « شخصی در راه به او برخورد و پرسید : در این طبق چیست؟ غلام چیزی نگفت. آن شخص به اصرار پرسید تا بداند زیر آن سرپوش که روی طبق کشیده‌اند چیست. غلام گفت: فلانی! اگر قرار بود که همه‌ی افراد بدانند در طبق چیست، دیگر سرپوش روی آن نمی‌کشیدند .

۳- مفهوم امانت

یکی از خصایل اخلاقی انسان که دارای ارزش و اهمیت فوق العاده‌ای است، امانت و امانت داری است . امانت در فرهنگ لغت، دارای معانی مختلفی است؛ پاس داری، حفاظت، امنیت، امان، مواظبت، مراقبت، رازداری، نگه داری، آسایش و آرامش روح و جان از جمله معانی امانت است . . امانت در نظر اسلام، از ارزش و جایگاه والایی برخوردار است، به طوری که در نمونه های فراوانی از سفارش ها و توجهات الهی قرآن و احادیث و روایات ائمه معصومین(ع) به چشم می خورد . خداوند در قرآن نسبت به حفظ امانت و سپردن آن به دست صاحبانشان می فرماید:

ان الله يامرکم ان تودوا الامانات الی اهلها... خداوند به شما فرمان می دهد که امانت ها را به صاحبانش بدهید.

۴- انواع امانت در اسلام

در فرهنگ اسلام امانت به دو چیز اطلاق می شود :

الف) تکالیف بندگی

ب) مال سپرده شده

الف- تکالیف بندگی:

این نوع امانت، نمونه های گوناگونی دارد که به آن ها اشاره می شود:

اعضا و نیروهای وجود انسان: تمام اعضا و جوارح توانایی ، استعداد ، نیروها و محرکه وجودی انسان نعمت‌هایی هستند که به صورت امانت در اختیار انسان قرار گرفته اند و بر ایشان است که از این امانت ها به طریقی شایسته و نیکو در راه رضای خدا و اطاعت کردن از او به کار گیرد و از بندگی شیطان و اسیر وسوسه های او شدن دست بردارد .

نمونه هایی از امانات: زبان به عنوان یکی از امانات الهی وظیفه دارد سخنان حق را بگوید و از گفتن سخنان لغو و بیهوده خودداری کند .

زبان آمد از بهر شکر و سپاس

به غیبت نگردانش ای حق شناس

یکی دیگر از امانات انسان، گوش است که باید از آن در راه شنیدن سخنان حق و غیر حرام استفاده کرد و از شنیدن سخنان باطل و ناروا دوری گزید .

چشم نیز باید از دیدن منظره های گناه آلود و فسادانگیز که تیری از تیرهای شیطان است، فرو بندد و در عوض مناظر و آیات عبرت انگیز را نظاره کند .

هان ای دل عبرت بین از دیده نظر کن هان

ایوان مدائن را آیینه عبرت دان

دست و پا، دو امانت دیگر الهی هستند که در اختیار انسان قرار گرفته است که از هر کدام باید در کارهای خیر و عام المنفعه بهره جست و از رفتن به مجالس فساد و عیاشی دست داشتن در کارهای غیر اخلاقی و شرعی خودداری کرد .

راز مردم: رازهای مردم نیز امانت اند و هیچ فردی حق ندارد بدون مصلحت خاص، اسرار دیگران را به هر طریقی فاش نماید .

ب: مال سپرده شده

منظور از مال سپرده شده، اموال و دارایی ها و احوانا اشیایی است که به انسان امانت داده می شوند و او باید از این امانت ها به نحو احسن نگه داری کند. به چند نمونه از انواع امانت از نوع مال سپرده شده اشاره می شود .

نامه ها و پیغام ها:

فرد امین باید در حفظ و نگه داری اسرار، مطالب و نوشته های دیگران کوشا باشد و آن را از دسترس بیگانگان هرزه و سودجو دور نگاه دارد .

اجناس و کالاها: فرد امین موظف است از وسایلی که به او سپرده می شود همانند جان خویش مواظبت کند و بدون رضایت فرد امانت دهنده به اموالش دست نزند و آن ها را خراب نکند .

بیت المال مردم: از مهم ترین امانت ، بیت المال مردم است. میز، کلاس، آب، برق، وسیله های نقلیه عمومی و هزاران وسیله دیگر همگی از اموال عمومی هستند که نزد همه به امانت سپرده شده است.

آثار اجتماعی امانت داری:

- جلب اعتماد اقشار جامعه

- احساس مسئولیت عمومی

- حفظ اسرار و اطلاعات کشور

امانت داری اجتماعی موجب می شود تا سیاست ها و طرح ها و نقشه های حکومتی که جنبه محرمانه و سری دارند، از دست برد بیگانگان و منافقان و جاسوسان در امان باشد.

بخش ۲ - اسرار و انواع آن:

اسرار یا رازها را می توان به سه دسته تقسیم نمود:

الف- اسرار شخصی

ب- اسرار اجتماعی

ج- اسرار تشکیلاتی - حکومتی

۱- رازداری شخصی

هرکس از نظر اخلاقی و عملی ، خصوصیات و اطلاعاتی دارد که خصوصی بوده و تمایلی به افشا آنها نزد سایرین ندارند ، و دیگران نمی بینند و از آن اطلاعی ندارند، این ویژگیها، رازهای شخصی انسان محسوب می شود، چنان که کارهای زشتی که از فرد سرزده و یا مسائل سرّی که در منزل دارد، جزو رازهای فرد به حساب می آید. حال سخن در این است که آیا انسان می تواند رازهایش را برای دیگران بازگو کند؟

انسان عاقل سینه خود را صندوقچه اسرارش قرار می دهد و از طریق رازداری ، خود را از پیامدهای ناگوار افشای اسرار، مصون می دارد .
امام علی (ع) می فرماید:

سِرُّكَ اسِيرُكَ، فَإِنَّ افْشِيَتَهُ صَرَتْ اسِيرَهُ

راز تو، مادامی که آن را بر ملا نکردي ، اسیر توست ، ولی اگر آن را فاش کردی تو اسیرش می شوی.

راز خود هرگز مگوی با یار خود یار را یاری بود از یار یار اندیشه کن.

نقش رازداری شخصی در موفقیت

هرگاه انسان هدفی را دنبال می کند، لازم است اطراف و جوانب آن را مخفی بدارد تا به نتیجه مطلوب برسد، آنگاه اگر افشای آن بی ضرر بود، می تواند آن را فاش سازد، ولی اگر کارش استحکام نیافته و به نتیجه نرسیده باشد، آن را بازگو کند، سنگ اندازیهایی نمی گذارد او به هدفش برسد.

امام صادق (ع) می فرماید:

لا تُطْلِعْ صَدِيقَكَ مِنْ سِرِّكَ إِلَّا عَلَى مَالٍ اَطَّلَعَ عَلَيْهِ عَدُوُّكَ لَمْ يَضُرُّكَ فَإِنَّ الصَّدِيقَ قَدْ يَكُونُ عَدُوًّا يَوْمًا مَّا؛
دوست خود را از رازهای شخصی خود آگاه مساز، مگر درباره اموری که اگر دشمنت از آنها آگاهی یافت ، زیانی برای تو نداشته باشد؛

زیرا چه بسا دوست انسان روزی دشمن او گردد و چون نقاط ضعف را می داند، با آن انسان را بکوبد .

به همان مقدار که رازداری شخصی در موفقیت انسان ، نقش دارد، افشای رازهای شخصی نیز موجب ناکامی انسان در رسیدن به هدفها می شود و موجبات پشیمانی انسان را فراهم می سازد .

۲- رازداری اجتماعی منظور از رازداری اجتماعی ، حفظ اسرار مردم در مسائل اجتماعی ، سیاسی و ... و بیان

نکردن نقطه ضعف های آنها در این زمینه است.

افشای اینگونه رازها جایز نیست ، ولی چنانچه اسرار اجتماعی و سیاسی افراد از قبیل اشاعه فحشا، تشکیل باندهای فساد و تباهی و این گونه کارهای خلاف باشد، نزد مسؤولین امر جهت اتخاذ تصمیم و اقدامات لازم ، مانعی ندارد و چه بسا ضروری باشد.

در مسائل اطلاعاتی ، امنیتی نیز افشای اسرار دیگران در اجتماع و برای مردم جایز نیست ، بلکه گاهی زیان آور است ، ولی اگر این اسرار از اموری باشد که کتمان آن خطری را متوجه نظام می کند، لازم است نزد مراجع صلاحیتدار بازگو شود و سکوت در مقابل آن جایز نیست.

بنابراین ، حفظ اسرار اجتماعی دیگران ، (جز در مواردی که افشاگری مهمتر و ضرورتر است) لازم می باشد، بویژه از ناحیه کسانی که زودتر و بیشتر از دیگران رازها در اختیارشان قرار می گیرد، مانند کسانی که در رابطه با امنیت داخلی یا خارجی کار می کنند و یا کسانی که در قسمت جذب و گزینش نهادها، ادارات و سایر مراکز هستند و درباره نیروهایی که می خواهند به کار بگیرند، اطلاعاتی کسب می کنند .

۳- رازداری تشکیلاتی - حکومتی

رازهای تشکیلاتی، حکومتی و حفظ آنها در بقای نظام مؤثر است. این بخش مورد ابتلای نیروهای اطلاعاتی و همه مردم است و بایستی در این زمینه هوشیاری و دقت کافی به خرج داده، از افشای مطالب مورد علاقه و توجه دشمن و سرویس های بیگانه خودداری نماییم.

حفظ این نوع رازها به مراتب مهمتر از سایر اسرار است. از این رو، پیامدهای افشای آن نیز ناگوارتر و زیانبارتر از سایر رازهاست. رازداری حکومتی از دیدگاه اسلام یکی از اصول مهم اخلاق اطلاعاتی است که می توان به وسیله آن امکان بسیاری از زیانها از ناحیه دشمن را سلب و همواره ابتکار عمل را در دست داشت.

۴- حریم خصوصی افراد:

حریم خصوصی: قلمرویی از زندگی شخصی فرد است که انتظار دارد دیگران بدون رضایت یا اعلام قبلی وی یا به حکم قانون یا مراجع قضایی آن را نقض نکنند؛ از قبیل حریم جسمانی، وارد شدن، نظاره کردن، شنود و دسترسی به اطلاعات شخصی فرد از طریق رایانه، تلفن همراه، نامه و ...

۵- برخی موارد مجاز افشای راز:

افشای راز دیگران در پاره ای از موارد مجاز شمرده شده است که برخی از آنها را در زیر می خوانیم :

الف - دادخواهی

فردی که از ناحیه دیگری مورد ستم قرار گرفته، برای دادخواهی ناگزیر است آن ظلم را به مراکز صلاحیتدار و یا مسؤؤل بالاتر گزارش دهد تا به موضوع رسیدگی واز تضييع حقدش جلوگیری به عمل آید.

قرآن مجید درباره حق دادخواهی مظلوم از ظالم می فرماید:

لَا يُحِبُّ اللَّهُ الْجَهْرَ بِالسُّوءِ مِنَ الْقَوْلِ إِلَّا مَنْ ظَلَمَ وَ كَانَ اللَّهُ سَمِيعاً عَلِيماً

خداوند دوست ندارد کسی با سخنان خود، بدی های دیگران را اظهار کند، مگر آن کسی که مورد ستم واقع شده باشد، خداوند، شنوا و داناست.

ب - استعانت بر نهی از منکر

در مواردی که انسان از منکری مطلع شود و بداند که اگر اقدامی نکند، این گناه شیوع پیدا کرده، زیان ناشی از آن به عموم مردم بر می گردد و خود نیز به تنهایی نتواند جلوی آن را بگیرد و ناگزیر باشد از مردم کمک بخواهد، باید چنین کند و با استمداد از دیگران مجرم را از کردار زشتش بازدارد، گرچه مردم از راز او باخبر شوند.

پ- بازگو کردن حقایق در ماموریت محوله به مقام مسؤل

۶- راههای رازداری

الف - حفظ اسرار، مایه شادمانی انسان است: انسان رازدار اختیارش باخودش است و خیر دنیا و آخرت در حفظ رازها نهفته است. این گونه فواید در رازداری موجب می شود که انسان اسرارش را حفظ و سفره دل را جلو هرکسی نگشاید و به فاش ساختن اسرار خود و دیگران نپردازد

ب- توجه به زیان و ضررهای افشای رازها

پ - خودداری از بیان تمام دانسته ها

ت - نصیحت در خلوت: اگر واقعاً در فردی صفت زشت و ناروائی وجود دارد با تذکرات دوستانه و به صورت پند و نصیحت

می توانیم او را از این خصلت ناپسند بازداریم، بلکه در برخی موارد نیاز به گفتن هم ندارد زیرا که با کردار و رفتار صحیح خود

می‌توانیم او را نسبت به عمل زشتش آگاه نمائیم.

در گفتن عیب دگران بسته زبان باش

با خوبی خود عیب نمای دگران باش

ث – حفظ زبان: یکی از عوامل اصلی افشاگری، زبان است، خیلی از گناهان توسط زبان انجام می‌شود، متأسفانه خیلی از افراد از کنترل زبان خود عاجز هستند

البته افشاگری همیشه با زبان نیست، بلکه گاهی مواقع با نوشتن بیانیه در فضای مجازی و مطبوعات است، برای حل این معضل باید تقوا و ترس از خدا را در خود و دیگران تقویت کنیم.

ج – پرهیز از کینه و انتقام: برخی از افشاگری‌ها به خاطر کینه و اختلافات شخصی است، مثلاً برای اینکه از کسی که کینه دارد انتقام بگیرد، عیوب او را جمع می‌کند و در وقت مناسب اسرار و عیوب شخصی او را افشاء می‌کند تا آبروی او را ببرد، کینه یک بار اضافی بر روح است و اثرات روحی و روانی زیادی به دنبال دارد، سعی کنیم این صفت رذیله را در خود از بین ببریم؛

۷- برخی پیامدهای افشا اسرار:

اطبا و جراحان و ماماها و داروفروشان و کلیه کسانی که به مناسبت شغل یا حرفه خود محرم اسرار می‌شوند، هر گاه در غیر از موارد قانونی، اسرار مردم را افشا کنند، از سه ماه تا یک سال و یا به یک میلیون و پانصد هزار تا شش میلیون ریال جزای

تقدیمی، محکوم می‌شوند. (بخشی از مجازات تعیین شده)

در برخی مواقع نامه یا گزارش محرمانه ای درباره موضوع یا یکی از کارمندان سازمان‌ها که باید به شکل محرمانه باقی بماند، در اختیار خود فرد قرار داده می‌شود و این امر برخلاف قانون است و علاوه بر افشای اسرار، موجب افشای منابع اخبار و اطلاعات می‌شود و تبعات زیادی در پی خواهد داشت. لزوم حفظ اسرار دیگران از حقوق عامه محسوب می‌شود و مرجع قضایی، مدعی العموم و حافظ حقوق عمومی است.

پیامدهای زشت بیهوده گویی

۱- تباه شدن عمر: کمترین زیان کلام بیهوده برای شخص گوینده، تباه شدن عمر اوست که بزرگ‌ترین سرمایه زندگی او شمرده می‌شود؛ چرا که انسان می‌تواند از این بخش زندگانی، برای جهان آخرت خود توشه بردارد ولی با گفتن سخنان بیهوده هیچ فایده دنیوی و اخروی به او نرسیده، فرصت از بین می‌رود.

۲- حقارت در اجتماع: سخن انسان نشانه شخصیت درونی اوست، پس اگر گفتار او بی‌فایده و بیهوده باشد، شخصیت او نیز نزد دیگران حقیر خواهد شد.

امام علی(ع) می‌فرماید: سخن بگویند تا شناخته شوید، همانا(شخصیت) انسان در پشت زبانش پنهان است.

۳- زمینه سازی برای گناهان زبانی: سخن بیهوده، زمینه ورود انسان به وادی گناهان زبان را فراهم می‌سازد؛ زیرا بیهوده گویی از شهوت کلام سرچشمه می‌گیرد و این اشتها به سخن گفتن خطرهایی چون غیبت، دروغ، تهمت و... را در پی دارد. پیامبر اسلام(ص) می‌فرماید: «کسی که بسیار سخن گوید، خطایش فراوان می‌شود و کسی که خطایش فزونی یابد، گناهانش بسیار می‌گردد و کسی که گناهانش فراوان شود، دوزخ برای او بهتر است.»

۴- از دست دادن امور مفید: هنگامی که انسان به امور بی فایده سرگرم می شود از آنچه مفید و سودمند است، باز می ماند

اما علی(ع) فرموداند: «هر کس خود را به چیزی که به کارش نیاید سرگرم سازد آنچه را که به کارش آید از دست می دهد.»

۵- نابودی خرد: عقل، انسان را به پیشرفت و کمال فرا می خواند، سرگرم شدن به امور زاید و بی فایده حرکتی در جهت خلاف دستور عقل بوده، موجب نابودی آن می شود.

امام علی(ع) می فرماید: «ضایع شدن عقل ها در جستجوی کارهای زاید است»

۶- قساوت قلب: دوری از یاد خدا دل را سخت می کند و حاصل بیهوده گویی و زیاده گویی در آنچه که فایده ندارد و به کار نیاید، کاهش ذکر خدا و سرانجام آن، قساوت قلب است.

رسول خدا(ص) می فرماید:

«سخن در غیر یاد خدا را زیاد نکنید، همانا سخن بسیار در غیر یاد خدا، دل را سخت می کند.»

درمان بیهوده گویی از دو راه علمی و عملی ممکن است:

۱- راه علمی: دقت در پیامدهای سخن بی فایده و یادآوری مستمر آنها، سبب ترک این عادت ناشایست می شود، آن گاه که انسان به اهمیت نقش سخن در زندگی آگاه شود، دیگر به گفتار بی فایده روی نخواهد آورد
امام صادق(ع) به نقل از رسول خدا(ص) می فرماید:

«هر کس جایگاه سخنش را در میان رفتارش بشناسد، گفتارش جز در امور مفید، کم می شود»

۲- راه عملی: سرگرم شدن به کارهای مفید و سودمند کوششی مناسب برای ترک عادت بیهوده گویی است؛ زیرا پرداختن به بیهوده گویی انسان را از کارهای سودمند بازداشته است، پس برای ترک آن باید خلافت عمل کرد.
پرداختن به ذکر، دعا، مسایل علمی و ارشاد و تربیت و تلاش برای کسب روزی حلال از جمله اموری است که انسان را از بیهوده گویی دور می سازد.

بخش ۳- رازداری از منظر قرآن ، روایات و سیره معصومین و...

افشاکری از منظر قرآن

با توجه به برخی از آیات قرآن مجید ، افشاکری نسبت به امور پنهانی و اسرار شخصی و نظامی مسلمین حرام است، قرآن مجید می فرماید: **يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَخُونُوا اللَّهَ وَالرَّسُولَ وَتَخُونُوا أَمَانَاتِكُمْ وَأَنْتُمْ تَعْلَمُونَ**؛ ای کسانی که ایمان آورده اید، (با مخالفت احکام دین) به خدا و فرستاده او خیانت نورزید و در امانت های خلقی و خالقی خیانت نکنید .
در حدیث از پیامبر (صلی الله علیه و آله) نقل شده: **ثَلَاثٌ مَنْ كُنَّ فِيهِ كَانَتْ مُنَافِقًا - وَ إِنْ صَامَ وَ صَلَّى وَ زَعَمَ أَنَّهُ مُسْلِمٌ مَنْ إِذَا انْتُمِنَ حَانَ وَ إِذَا حَدَّثَ كَذَبَ وَ إِذَا وَعَدَ أَخْلَفَ**؛ نشانه منافق سه چیز است هر چند روزه بگیرد و نماز بخواند و خود را مسلمان بداند: هنگامی که امانتی نزد او بگذارند خیانت می نماید، هنگام سخن دروغ می گوید، و به هنگامی که وعده می دهد تخلف می کند.

افشاکری از منظر روایات

در روایات زیادی از افشای اسرار جامعه اسلامی و رازهای مردم نهی شده است، مثلا در کتاب کافی باب مستقلی با عنوان باب الاذاعه افشای اسرار اهل بیت علیهم السلام است .

ائمه و رازداری

اسلام، هم به حفظ اسرار خودمان سفارش کرده و هم به حفظ اسرار دیگران. در روایات توصیه شده که اسرار زندگی خصوصی خود را حفظ کنید! چرا که افشای آن گاهی منشأ حسد، کینه توزی و رقابت های ناسالم می گردد و انسان مورد تهاجم افراد تنگ نظر و کینه توز واقع می شود و مصالحش به خطر می افتد.

امام علی علیه السلام فرمود: «سِرُّكَ سُرُورُكَ اِنْ كَتَمْتَهُ وَ اِنْ اَدَعْتَهُ كَانَ نُبُورَكَ». سرّ تو مایه سرور و خوشحالی تو است، به شرط آنکه آن را کتمان کنی، و اگر آن را افشا کنی، (چه بسا) مایه هلاک تو می شود.

و فرمود: «جُمِعَ خَيْرُ الدُّنْيَا وَ الْاٰخِرَةِ فِي كِتْمَانِ السِّرِّ وَ مَصَادِقِهِ الْاٰخِيَارِ وَ جُمِعَ الشَّرُّ فِي الْاِذَاعَةِ وَ مُوَآخَاهِ الْاَشْرَارِ». تمام خیر دنیا و آخرت در دو چیز جمع شده: در راز داری و دوستی با نیکان، و تمام بدی ها در دو چیز جمع است: افشای سر و دوستی با بدان

همچنین امیر مومنان علیه السلام فرمود: «مَنْ اَفْشَى سِرّاً اِسْتَوْدِعَهُ فَقَدْ خَانَ» هر کس سری را که به او سپرده شده، فاش کند، خیانت کرده است.

حدود راز داری اخلاقی:

آیا در مکتب اهل بیت علیهم السلام به هیچ عنوان شایسته و پسندیده نیست که اسرار خود را به کسی بگوییم؟ یا این که «رازداری» حد و اندازه گیری دارد و در برخی موارد می توان راز خود را به دیگری گفت؟

در پاسخ می گوییم: ائمه اطهار علیهم السلام برخی موارد را استثنا کرده اند؛ از جمله امام صادق علیه السلام فرمود: «لَا تُطْلِعْ صِدِّيقَكَ مِنْ سِرِّكَ اِلَّا عَلَى مَا لَوْ اَطَّلَعْتَ عَلَيْهِ عَدُوَّكَ لَمْ يَضُرَّكَ فَاِنَّ الصِّدِّيقَ قَدْ يَكُونُ عَدُوّاً يَوْمًا مآ؛ دوستت را بر آن مقدار از اسرار آگاه ساز که اگر دشمنت هم آن را بداند، به تو زیان نرساند؛ شاید دوست نیز روزی دشمنت گردد».

فصل دوم: حفاظت اسناد

مقدمه:

حراست یکی از عمده ترین وظایف ذاتی بشر است. و نه تنها انسان، بلکه سایر موجودات زنده نیز از «خود» و آنچه که متعلق به «خود» است حراست می کنند.

نگاهی به ابزار دفاعی آنها اعم از گریز، درگیری، اعمال فریب و نیرنگ، پرواز یا همسانی با محیط، تداعی کننده حراست از جان خویش است.

انسان نیز با خلق سخت افزاری چون قفل و صندوق نسوز و نرم افزاری چون دستورالعمل و بخشنامه در جهت حراست از دارایی های خویش تلاش می کند.

اسناد و مدارک طبقه بندی شده هر کشور جزء دارایی های با ارزش آن محسوب شده و حفاظت از آنها بر مبنای دلایل عقلی و قانونی اجتناب ناپذیر بوده و یکی از وظایف واحدهای مسئول در این رابطه می باشد، زیرا افشای آنها و دسترسی افراد غیر مجاز بویژه دشمنان، رقبا و کسانی که به هر دلیلی به دنبال سوء استفاده از آن اسناد و اطلاعات می باشند ضربات جبران ناپذیری بر اساس حکومت، منافع ملی، منافع کشور و یا یک سا زمان وارد می کند.

اقداماتی که برای حفاظت اسناد به عمل می آید به مقدار زیادی به سطح طبقه بندی حفاظتی آن بستگی دارد هر چه سطح

طبقه بندی سندی بالاتر باشد ، برای حفاظت آن باید تلاش بیشتری به عمل آید . علاوه بر آن شرایط زمانی ، مقدمات قانونی و سازمانی، زمان و مکان نگهداری نیز از جمله عواملی هستند که در این رابطه نقش دارند.

ارزش اطلاعات:

اگر قبول کنیم که اطلاعات به مثابه آدرس‌های گنج می باشد پس باید پذیرفت که ارزش مادی دارند و با پول تعویض می گردند.

مثال: آیا پیشنهاد رقبا برای برنده شدن در یک مناقصه برای فردی که قصد برنده شدن در آن مناقصه را دارد در حکم آدرس یک گنج چند میلیون تومانی نیست؟

حفاظت چیست ؟ حفظ و نگهداری اهداف حفاظتی در مقابل تهدیدات و خطرات طبیعی و مصنوعی.



تعریف حفاظت اسناد و مدارک: اقداماتی است به منظور نگهداری اسناد و مدارک در مقابل خطرات طبیعی و مصنوعی. و جلوگیری از دسترسی افراد غیر مجاز.

تعریف سند: سند هرگونه نوشته، نوار، فیلم، نقشه و شی است که حاوی نکته های اطلاعاتی باشد.

تعریف اسناد از نظر حقوقی و قضایی: از نظر حقوقی سند یکی از وسایل اثبات حق است. به موجب ماده ۱۲۸۴ قانون مدنی ایران سند عبارت است از « هر نوشته ای که در مقام دعوی یا دفاع قابل استناد باشد». منظور از نوشته ها یا خط علامتی است که در روی صفحه خود را نشان دهد و مبین پیام یا مفهوم خاصی باشد.

سند از نظر قانون سازمان اسناد ملی ایران

عبارت است از «کلیه مراسلات»، دفاتر، پرونده ها، عکس ها و... سایر اسنادی که در دستگاه دولت تهیه و صادر و یا دریافت شده و به طور مداوم یا غیر مداوم در تصرف دولت بوده، از لحاظ اداری، اقتصادی، قضایی، سیاسی، فرهنگی، علمی و تاریخی به تشخیص سازمان اسناد ملی ایران دارای ارزش نگهداری دایمی باشد

مدیریت گردش اسناد

سند مانند انسان سه مرحله را طی می کند: تولد - حیات - پایان استفاده (امحا) ، مدیریت فردی و سازمانی در این سه مرحله بر روی اسناد از اقدامات اساسی در حفظ و نگهداری اسناد است.

گردش اسناد

- الف - تهیه و تولید سند (تولد)
- ب - انتشار و بهره برداری و بایگانی (حیات)
- پ - امحا سند (پایان)

انواع سند:

۱- از نظر اطلاعاتی:

الف-عادی

ب-طبقه بندی شده

۲- از نظر گردش اسناد

الف-سنتی

ب-دیجیتالی

سند: هر شی، مدرک، وسیله و... که اطلاعاتی را ارایه نماید سند نامیده می شود. اگر این اطلاعات دارای ارزش حفاظتی باشد به آن سند محدود یا طبقه بندی می گویند. اگر سند دارای پیوست و ضامته باشد به آن سند مرکب می گویند.

برخی تهدیدات اسناد و مدارک

آتش سوزی - سرقت - تخریب - جعل و تزویر - جاسوسی و دستبرد عوامل بیگانه داخلی و خارجی - چاپ و نشر غیر مجاز - دسترسی افراد غیر مجاز - سوء استفاده - تداخل اسناد و بایگانی غلط - خوردگی توسط حشرات موذی - عدم رعایت حفاظت گفتار توسط کارکنان. نفوذ به شبکه و اینترنت و هک. ارسال از طریق دور نگار و سیستم مخابراتی آسیب پذیر، اقدام کننده هایی که آموزش ندیده اند و...

شرایط دسترسی:

الف - نیاز به دانستن: به این مفهوم که اگر فرد از آن دانائی اطلاع نداشته باشد قادر به انجام مأموریت خود نخواهد بود پس

برای انجام امور مربوطه نیاز به دانستن دارد. مانند ماشین نویسی که بدون اطلاع از متن یک سند قادر به تایپ آن نخواهد بود.

ب - داشتن صلاحیت امنیتی: هر فردی که نیاز به دانستن دارد، پیش از آن بایستی صلاحیت لازم در امور امنیتی را از یک مرجع ذیصلاح کسب کرده باشد. معنای این موضوع آن است که افراد نفوذی، خرابکار، سارق و وابسته به بیگانه قادر به ورود در پوشش کارمندی یا کارگری به مجموعه های خودی نباشند.

ج - آموزش: نیل به دو شرط نیاز به دانستن و صلاحیت امنیتی گرچه لازم است اما کافی نیست زیرا در صورتی که کارکنان، آموزش لازم برای حفاظت از اطلاعات کاربردی را نداشته باشند قادر به حراست از آن نخواهند بود.

مساله: آقای جلالی در ساعت ۱۰ صبح در حالی برای پاسخگویی به تلفن راه دور اتاق خود را ترک کرد که یک سند محرمانه بر روی میزش باقی ماند. او پس از ۵ دقیقه مراجعه در مییابد یک ارباب رجوع در اتاقش بر روی صندلی نشسته است آیا میتوانید وظایف امنیتی آقای جلالی را در جهت حراست از سند محرمانه مذکور بیان نمائید؟

اختیارات و شرح وظایف

۱- **مدیران** : مسئول تأمین و حصول اطمینان از حفاظت اسناد و مدارک طبقه بندی شده هستند.

۲- **پرسنل دستگاه**: پرسنلی که دسترسی به اسناد و مدارک طبقه بندی شده دارند باید :

الف) با کلیه ضوابط و مقررات تأمینی آشنایی داشته باشند..

ب) از اطلاعات و اسناد طبقه بندی شده موجود حفاظت و حراست نماید.

ج) همواره از نحوه حفاظت از اطلاعات برابر روش های آیین نامه های مربوطه اطمینان حاصل نمایند.

۳- **حراست سازمان**: موظفند بر حسن اجرای مقررات تأمینی و حفاظت از اسناد و مدارک طبقه بندی شده بطور مستمر نظارت داشته باشد.

طبقه بندی:

تعریف طبقه بندی: دو تعریف مفهومی بر مبنای دو لغت خاص برای طبقه بندی وجود دارد:

۱- تعیین ارزش حفاظتی اسناد به منظور در نظر گرفتن اقدامات حفاظتی برای آنها.

۲- تعیین میزان خسارت ناشی از افشای غیر مجاز اسناد.

معلوم شد که دو لغت خاص عبارتند از :

۱- ارزش اطلاعاتی

۲- خسارت ناشی از افشا

طبقه بندی چیزی به جز ارتباط میان همین دو لغت نیست، زیرا آنچه که ارزش بیشتری داشته باشد در صورت افشاء غیر مجاز می تواند خسارت فراوانتری وارد نماید. لاجرم ارزش بالاتری خواهد داشت. اسناد و مدارک طبقه بندی باید در محل مطمئن نگهداری شوند. (اسناد سری و به کلی سری فقط در فایل کابینت رمزدارنگهداری شود.

انواع طبقه بندی اسناد

۱- بکلی سری TOP SECRET

۲- سری SECRET

۳- خیلی محرمانه VERY CONFIDENTIAL

۴- محرمانه CONFIDENTIAL

بسته بندی و ارسال اسناد محرمانه:

طبقه بندی محرمانه : برای سندی به کار می‌رود که انتشار آن بین عموم آزاد نبوده و افشای آن باعث بروز اختلال در بخشی از سیستم‌های داخلی یک سازمان می‌شود.

نحوه ارسال اسناد محرمانه به خارج از سازمان

- ۱- یک پاکته کردن.
- ۲- درج دو مهر طبقه‌بندی محرمانه بر پشت پاکت.
- ۳- الصاق یک عدد لاک و مهر بر روی درب پاکت.

بسته‌بندی اسناد خیلی محرمانه:

طبقه بندی خیلی محرمانه : این طبقه بندی برای اسنادی به کار می‌رود که افشای غیرمجاز آن به بخشی از منافع کشور لطمه وارد نماید.

- ۱- دو پاکته کردن.
- ۲- درج دو عدد مهر طبقه بندی خیلی محرمانه بر پشت پاکت بیرونی.
- ۳- الصاق سه عدد لاک و مهر بر روی درب پاکت داخلی.

بکلی سری: در مورد اسنادی به کار می‌رود که افشای غیر مجاز آن به امنیت ملی کشور ضرر و زیان جبران ناپذیر به امنیت ملی و سیستم دفاعی کشور وارد می‌سازد.

سری: در مورد اسنادی به کار می‌رود که افشای آن امنیت ملی کشور (منافع عمومی، سیستم دفاعی، روابط خارجی و...) را به مخاطره می‌اندازد.

بسته بندی اسناد سری و به کلی سری:

- دو پاکته کردن.
- درج دو عدد مهر سری یا بکلی سری در بالا و پائین پشت پاکت بیرونی.
- الصاق پنج عدد لاک و مهر بر روی درب پاکت داخلی.
- الصاق فرم شماره ۳ به پاکت مذکور.
- ارسال پاکت با پیک انسانی ویژه با صلاحیت.

فرم شماره ۳ چیست؟

این فرم به دو منظور مورد بهره‌برداری قرار می‌گیرد:

- اطمینان از وصول سند
 - تعیین مشخصات اولین فردی که از مفاد سند آگاه می‌شود.
- توجه:** اگر ارسال اسناد طبقه بندی در داخل سازمان واحد انجام می‌گیرد به نحو زیر اقدام می‌شود :
- اسناد سری و بکلی سری یک پاکت و سه لاک و مهر و دو علامت طبقه بندی.
- اسناد خیلی محرمانه و محرمانه یک پاکت بدون لاک و مهر (با دو علامت طبقه بندی).

افشا چیست؟

عرضه متن اطلاعات، اسناد و اخبار به صورت شفاهی یا کتبی یا به هر نحوی که امنیت سند به خطر بیفتد را افشاء گویند.

مثال: ماشین نویسی که پس از تایپ یک نامه، محتوای آن را برای دیگران بازگو کند، یا مینوت نامه را امحا نکند آن سند را افشاء نموده است.

انواع افشا:

- افشا مجاز: که چاره‌ای از آن نیست و برای ادامه امور اداری انجام می‌گیرد. مانند ارائه گزارش کار به مدیر رده بالاتر.
- افشاء غیر مجاز: که سبب سوخت اطلاعات شده و جرم تلقی می‌گردد.

مسئولین حفاظت اسناد:

- الف - مدیران و رؤسای قسمت‌ها.
- ب - کارکنان قسمت‌ها.
- ج - حراست مستقر در تأسیسات.

کارکنان قسمت‌ها:

هر یک از کارکنان که در مسیر شغلی خویش به اطلاعاتی دسترسی دارند موظف به حراست از آن نیز می‌باشند، این مسئولیت به روش‌های زیر قابل اعمال خواهد بود:

۱- **اقدام فردی:** انتقال فرهنگ مسئولیت‌پذیری امنیتی از منزل به محل کار مهمترین وظیفه‌ای است که یک فرد می‌تواند در راستای امور حراستی به انجام برساند. بدین معنی که همه ما در منازل خود حفاظت اسناد، حفاظت گفتار و سایر شیوه‌های حراستی غیرعامل را به انجام می‌رسانیم پس باید تلاش کنیم تا این اقدامات در صورت جمعی و کلی آن در ادارات نیز به انجام برسد و این موضوع بستگی به هر فرد از کارکنان دارد، زیرا تهدید، گرچه ممکن است بسیار کوچک باشد اما مانند سوراخ کف کشتی (علیرغم کوچکی) بالاخره منجر به غرق آن خواهد گردید. وظایف مسئولیتی افراد می‌تواند شامل اطمینان از عدم افشاء اطلاعات مکتوب، عدم دسترسی افراد غیر مجاز به اطلاعات، بازگو نکردن متون اسناد و اخبار نزد افراد غریبه و غیرمجاز، به منزل نبردن اسناد و مدارک دولتی و ... تا نظارت مستقیم به امحاء اسناد باطله محل کار باشد.

۲- **ارشاد دیگران:** تنها وجود یک تهدید که ناشی از سهل‌انگاری یکی از کارکنان باشد ممکن است منجر به افشاء غیرمجاز یک راز گردد به همین دلیل عناصر آگاه علاوه بر اقدامات فردی، دیگران را نیز هدایت نموده و به موقع با تذکری ساده از یک خطای بزرگ جلوگیری می‌نمایند و این امر، مفهوم امر به معروف یا نهی از منکر است.

۳- **حیطه بندی:** یعنی رعایت اصل نیاز به دانستن. تعیین مرزهای افقی و عمودی در مسیر گردش اطلاعات را حیطه بندی نامند. مسئولیت حیطه بندی ایجاب می‌کند ماشین نویسان متن نامه‌های تایپ شده را با یکدیگر مورد بحث و مشورت قرار ندهند (مرز افقی) و نیز مدیران همه آنچه که می‌دانند به کارشناسان نگویند مگر به قدر نیاز و ضرورت (مرز عمودی). حیطه بندی یعنی عدم افشاء اطلاعات شغلی در اماکن غیر شغلی مانند منازل. بطور کلی می‌توان حدود مسئولیت افراد در حیطه بندی را به موارد زیر خلاصه نمود:

- عدم افشاء اطلاعات نزد زیردستانی که نیاز به دانستن ندارند.
- عدم افشاء اطلاعات نزد همکارانی که نیاز به دانستن ندارند.
- عدم افشاء اطلاعات نزد افرادی که دسترسی شغلی ندارند.
- عدم افشاء اطلاعات نزد افراد خانواده.

حفاظت اطلاعات رایانه ای: اقداماتی است به منظور حفظ اطلاعات دیجیتالی، شبکه و رایانه ای در گستره سازمانی و

تعیین شرایط دسترسی به رایانه و چگونگی انتقال اطلاعات



-امنیت سخت افزاری

-امنیت نرم افزاری

-رمز ورود



رسانه های ذخیره ساز

► وسیله الکترونیکی که قابلیت ذخیره و پاک کردن اطلاعات را داشته باشد. (دیسک سخت ، فلش، سی دی و....

اطلاعات رسانه های ذخیره ساز

► به گونه ای امحا گردند که قابل باز یابی نباشند.

آیا به تامین امنیت رایانه و شبکه اندیشیده ایم؟



برخی تهدیدات و آسیب پذیری های اطلاعات:

۱- عوامل اطلاعاتی و سازمان های جمع آوری

۲- نفوذ گر ها، هکر ها و...

برخی اشتباه های کارکنان:

* ۱ - رعایت نکردن بخشنامه های حفاظتی

* ۲ - دریافت فایل از سایت های نامطمئن

* ۳ - عدم رعایت امنیت فیزیکی و ایجاد تسهیلات سرقت رایانه

* ۴ - ذخیره اطلاعات حساس در حافظه کامپیوتر منزل و ذخیره غیر ایمن.

ایمنی اسناد دیجیتالی:

* ۱ - کنترل تردد به محل سیستم رایانه ای

* ۳ - تفکیک اتاق های حاوی سیستم

* ۴ - تجهیز درب ورود و خروج به قفل و رمز و...

* ۵ - نگهداری نسخه های پشتیبان اطلاعات در محل دیگر و امن

* ۶ - استفاده از حافظه بیرونی (هارد اکسترنال) برای نگهداری و ..اطلاعات

- * ۷ - تجهیز سیستم به آنتی ویروس و ... (آخرین نسخه و قابلیت بروزرسانی
- * ۸ - تنظیم سیستم و عدم اجازه برای باز شدن اتوماتیک برنامه ها.
- * ۹ - عدم استفاده از نرم افزارهای مشکوک و اسکن نشده
- * ۱۰ - عدم اتصال به اینترنت
- * ۱۱ - استفاده از رمز عبور ،دیواره آتش و...
- * ۱۲ - عدم افشای کلمه عبور
- * ۱۳ - انتخاب کلمه عبور حداقل ۸ کاراکتر (تلفیقی از عدد
- * ۱۴-حروف بزرگ و کوچک ، نشانه ها
- * ۱۵ - کلمه عبور در حافظه ثبت شود و فقط یک نسخه در پاکت مهر و لاک شده تحویل مسئول نگهداری اسناد
- * حراست ،درصندوق مادر شود.
- * ۱۶ - عدم دانلود برنامه های رایگان از اینترنت
- * ۱۷ - رمز ورود را بیش از دو نفر ندانند
- * ۱۸ - تغییر رمز در صورت افشا
- * ۱۹ - تعمیر کیس در محل مطمئن یا در محل اداره
- * ۲۰ - عدم استفاده ازهر وسیله عمومی برای انتقال کیس برای تعمیر
- * ۲۱ - نگهداری هارد اکسترنال در محل امن
- * ۲۲ - ثبت مشخصات استفاده کنندگان اطلاعات در دفتر مخصوص
- * ۲۳ - اطلاعات طبقه بندی داخل حافظه داخلی رایانه ثبت نشود.
- * ۲۴ - تحویل و تحول هارد و سایر وسایل برابر دستورالعمل حراستی باشد.
- * ۲۵ -از سیستم عامل اورجینال استفاده شود.

برخی اطلاعات مورد نیاز سرویس های جمع آوری:

- متون قراردادها تا قبل از انعقاد
- صورتجلسات کمیسیون ها
- صورت نیازمندی بخش های عملیاتی
- ماموریت ها و وظایف هر قسمت
- نقاط حساس و آسیب پذیر
- علل نارضایتی کارکنان
- تاسیسات مهم اداری و عملیاتی
- آمار ،مشخصات و آدرس کارکنان
- طرح های حفاظتی و نگهداری تاسیسات
- برنامه های بازدید و سفرهای خارجی کارکنان و اطلاعات طبقه بندی ،محدود و اداری. و.....

انواع بایگانی:

الف: بایگانی متمرکز

ب: بایگانی پراکنده

ج: بایگانی راکد

نمونه هایی از فایل های نگهداری اسناد

برای بایگانی و نگهداری اسناد طبقه بندی شده شرایط ذیل لازم است:

الف) پیش بینی مکان حفاظت شده ترجیحاً در محل دبیرخانه محرمانه.

ب) استفاده از وسایل و ابزار و تجهیزات مطمئن و ایمن.

ج) محل مجهز به دوربین مدار بسته و حتی الامکان سیستم اطفاء حریق باشد.

د) استفاده از کارکنان واجد شرایط و تعیین صلاحیت شده.

روش نگهداری ونحوه تحویل و دریافت اسناد طبقه بندی شده:

الف) صندوق نسوز وسایل نگهداری اسناد (فقط برای اسناد طبقه بندی شده بکار برده شوند).

ب) از خارج کردن کلید محل نگهداری اسناد از محل کار خودداری گردد.

ج) مسئولین حفاظت از اسناد موظفند محلی برای نگهداری کلیدهای محل و وسایل بایگانی ایجاد کنند.

د) هرگونه تکثیر از کلیدهای مذکور ممنوع است. (در صورت لزوم با اخذ مجوز از حراست کل)

ه) در صورت مفقود شدن کلیدها باید در اسرع وقت قفل های مربوطه تعویض گردند.

و) واگذاری و در دسترس گذاردن کلید به افراد غیر مجاز ممنوع است.

ز) در صورت جابجایی کارکنان شاغل در بایگانی محرمانه، قفل ها تعویض و رمزهای تغییر یابد.

ح) کلید محل های نگهداری اسناد اعم از فایل ها، گاوصندوق، کمد و... در تمام مدت قفل باشند.

ط) در مواقع تعمیر و نظافت اتاق هایی که اسناد طبقه بندی در آنها نگهداری میشود باید کارمند مسئول حضور داشته باشد.

روش غلط بایگانی اسناد:

توجه: اطلاعات طبقه بندی در حافظه و هارد داخلی رایانه ها ، ذخیره نشود ، بلکه از حافظه ی خارجی (

اکسترنال هارد) استفاده و پس از خاتمه وقت اداری ، آنها در صندوق های نسوز مجهز به قفل و رمز نگهداری

گردند.

بایگانی دیجیتال اسناد:

عصر ارتباطات و استفاده از شبکه های رایانه های در جهان کنونی و استفاده از سیستم های مدیریت اسناد

الکترونیکی در تمام حوزه های علمی و فعالیت های اجرایی رشد قابل توجهی داشته است. استفاده از سیستم های

مدیریت اسناد الکترونیکی چه در حوزه اجرایی و چه در حوزه تحقیق و پژوهش مزایای بیشماری دارد که در روش

های سنتی بایگانی دستیابی و استفاده از آنها بسیار دشوار به نظر می رسد.

بایگانی پرونده های به صورت سنتی مشکلات متعددی دارد. از جمله:

▶ نیاز به فضای زیاد که با توجه به ارزش ساختمان و کمبود فضای فیزیکی ساخت و نگهداری بایگانی هزینه

بسیار زیادی به سازمان تحمیل می کند.

- ▶ استهلاک و آسیب رسیدن به اسناد به مرور زمان و بر اثر استفاده مکرر
- ▶ رسیدن آسیب به پرونده ها به دلیل شرایط نگهداری نامناسب و یا اثرات محیطی.
- ▶ عدم امنیت فیزیکی بایگانی و امکان پذیر بودن دسترسی افراد غیر مجاز به اسناد و مدارک.
- ▶ هزینه های بالای نیروی انسانی در مراکز بایگانی.
- ▶ دسترسی و جستجوی زمان بر.
- ▶ عدم وجود گزارشات مناسب از وضعیت مراجعات به یک سند.
- ▶ عدم امکان دسترسی سریع و بی واسطه مدیران، محققان و سایر. به اسناد در صورت نیاز

در کل استفاده از روش بایگانی سنتی به ویژه در مورد پرونده ها به میزان بسیار زیادی باعث کاهش بهره وری در روند کاری می گردد. هرچند برابر آیین نامه حفاظت اسناد و مدارک، نگهداری اصل بسیاری از مدارک تا مدت زمانی که در قانون مشخص شده لازم است اما فناوری اطلاعات و روشهای نوین آرشیو الکترونیک باعث گردیده دیگر برای انجام امور روزمره و نگهداری پرونده های قدیمی نیازی به مراجعه به اصل اسناد نباشد. نکته حائز اهمیت اینکه در بایگانی دیجیتالی باید نسخه پشتیبان از مدارک تهیه شود و مقررات نگهداری مدارک نیز مد نظر واقع گردد. حفاظت از رایانه و سیستم شبکه - دسترسی کارکنان به برنامه ها یا پایگاه های داده حاوی اطلاعات حساس باید به طور منظم بررسی شود. و هر فردی به اتاق های حاوی کیس و اطلاعات رایانه ای تردد نداشته باشد و هنگام تعمیرات تعمیرکار با صلاحیت تحت نظارت نماینده فنی حراست در محل حضور داشته باشد. و راه اندازی سیستم شبکه سازمان توسط افراد و شرکت هایی که صلاحیت آنها مورد تایید سازمان حراست قرار گرفته انجام و راه اندازی شود.

انتخاب رمزهای عبور منحصر به فرد - برای حصول اطمینان از کیفیت کلمه عبور، حداقل از هشت کارکتر با ترکیبی از اعداد و حروف بهره بگیرید. هرگز از کلمات عبور یکسان برای همه حساب های خود استفاده ننمایید.

مزایای اجرا شدن بایگانی دیجیتالی:

پس از اجرای کامل پروژه بایگانی دیجیتالی می توان از مزایایی همچون موارد زیر بهره برد:

- ▶ تعیین سطوح دسترسی به پرونده ها
- ▶ جستجوی پیشرفته و دسترسی سریع و آسان به اوراق و اسناد بایگانی شده
- ▶ استفاده از اسناد بایگانی به صورت همزمان توسط چندین نفر از طریق شبکه داخلی سازمان. البته سطح دسترسی و رمز عبور هریک از کارکنان بایستی تعیین و تعریف شود.
- ▶ امکان به روز رسانی سیستم بایگانی.
- ▶ عدم از بین رفتن و آسیب اسناد در حین گردش کار.
- ▶ سازماندهی و مدیریت بر نحوه نگهداری و دسترسی به اسناد.
- ▶ امکان نگهداری نسخه های پشتیبان از اسناد و مدارک.
- ▶ امکان ساخت و ایجاد انواع گزارشات از لیست پرونده ها و اسناد موجود در آن
- ▶ پیگیری و کنترل دسترسی هر کاربر به هر سند و پرونده.

نگهداری ابزار کار:

۱- دستگاه ماشین نویسی: برخی از دستگاه‌های ماشین‌نویسی دارای ابزاری از قبیل نوار هستند که بصورت یک حافظه مخفی مطالب تایپ شده را درون خود نگهداری می‌کنند در این صورت حفاظت از اسناد حکم می‌کند که چنین نوارهایی هر روز از محل خود خارج و در همان صندوقها نگهداری شود و چنانچه نیاز به استفاده از نوار جدید پیش آمد به هیچ وجه نباید نوار قبلی را به شرکتهای ذیربط پس داد. زیرا یکدوره از اسناد تایپ شده در چنین نوارهایی وجود دارند.

۲- پرینترها: برخی از دستگاه‌های اسکنر، پرینتر، کپی پیشرفته و غیره غالباً دارای حافظه بوده و بعضاً تا دو هزار نسخه از مطالب کپی گرفته شده را در حافظه خود نگه می‌دارند. بدیهی است چنین دستگاههایی نیاز به سرویس داشته و در همین حالت سرویس کار قادر است ظرف مدت چند ثانیه حافظه را تعویض و بدین ترتیب اطلاعات فراوانی را به سرقت برد.

۳- رایانه‌ها: معضل اساسی نشت اخبار اداری استفاده از رایانه‌هاست. اکنون بیشترین اطلاعات به منظور طراحی، تایپ، پردازش، ذخیره سازی، حسابداری، انبارداری، تحویل و تحول و غیره به طور روزمره وارد می‌شوند.

سرقت اطلاعات رایانه ها:

- سرقت سخت افزار: به کرات گزارش شده است که در برخی از ادارات دولتی، هارد دیسک کامپیوتری به سرقت رفته است.

- اتصال به اینترنت: نفوذگرها قادرند با استفاده از سیستم های شبکه ای در زمانی اندک به رایانه‌های شخصی و اداری وارد شده و اطلاعات آن ها را به سرقت برند.

- عدم استفاده از رمز عبور: که سبب می‌شود هر فرد غیر مجاز از قبیل نظافتچی و ... در ساعات تعطیل ادارات قادر به روشن کردن و در نتیجه دسترسی به اسناد و اطلاعات موجود در کامپیوترها شوند.

راه چاره برای جلوگیری از معضلات فوق و نیز مشکلات دیگری که عنوان نشده آن است که:

اولاً: از رمزهای پیچیده متشکل از حروف و اعداد برای روشن کردن رایانه استفاده شود.

ثانیاً: سیستمی که در آن اطلاعات طبقه‌بندی ذخیره می‌شود به هیچ عنوان به اینترنت متصل نگردد.

ثالثاً: در پایان وقت اداری هارد دیسک کامپیوتر را برداشته و درون صندوق نسوز مجهز به قفل رمز قرار دهیم. (مانند اسناد طبقه بندی شده).

نگهداری در زمان ارسال و دریافت:

مسئولیت نگهداری اسناد در زمان ارسال، ایجاب می‌کند که اقدامات زیر در زمان ارسال و دریافت مورد توجه قرار گیرد:

▶ اسناد سری و بکلی سری بوسیله پیک مخصوص ارسال شوند.

▶ حق رمز و مخابره اسناد سری و به کلی سری را نداریم و برای شرایط خاص به مفاد آیین نامه مراجعه شود.

▶ ارسال و دریافت اسناد بوسیله فاکس، تلفن و شیوه‌های مخابراتی دیگر مانند ایمیل، امری ناپسند بوده و

امنیت را به خطر می‌اندازد لذا تنها تحت شرایط زیر مجوز لازم صادر می‌گردد:

۱- پیام دارای ارجحیت زمانی بالایی باشد.

۲- از سیستم کد و رمز استفاده شود.

دیرخانه رمز و محرمانه :

محلّی است که پیام‌ها و اسناد تهیه شده دارای طبقه بندی حفاظتی، برای ارسال به مقصد نهایی به آن جا هدایت می‌گردند.

اقدامات دبیرخانه: در مجموع می‌توان هفت نوع اقدام زیر را در دبیرخانه‌ها شمارش نمود:

- ▶ دریافت اسناد طبقه بندی، طبق لیست و براساس تحویل و تحویل.
- ▶ تعیین ترتیب حق تقدم ارسال بر اساس مهرهای ارجحیت اقدام سریع و عادی برای نامه‌ها و ارجحیت عادی، فوری، خیلی فوری و آنی برای پیام‌های رادیویی و تلفنی.
- ▶ پاکت گذاری نامه‌ها و اسناد بر اساس نوع طبقه‌بندی آنها (یک پاکت و دو پاکت).
- ▶ نصب لاک و مهر بر روی پاکت‌های درونی و درج آدرس‌های گیرنده و فرستنده و شماره و تاریخ بر روی پاکت بیرونی.
- ▶ دسته‌بندی پاکت محتوی اسناد بر اساس گیرندگان و تهیه لیست تحویل و تحویل.
- ▶ تحویل پاکت حاوی اسناد به پیک‌ها و دریافت نامه‌های وارده براساس لیست‌های مربوطه.
- ▶ شماره نامه‌های دریافتی را ثبت و پاکت‌های حاوی نامه را تحویل گیرندگان می‌نماید. و تقسیم آنها بر اساس گیرندگان ذیربط با ملاحظه طبقه‌بندی.
- ▶ هولوگرام‌های هات استمپ: به موجب آیین نامه حفاظت اسناد و مدارک طبقه بندی می‌توان بجای لاک و مهر از هولوگرام مخصوص روی پاکت‌های طبقه بندی استفاده نمود. و آن به هیچ وجه از سطح مورد نظر جدا نمی‌شود
- ▶ روی فویلی نازک، به صورت رول ثبت می‌شود و بر روی یک حامل (Carrier) مثل پلی استر قرار می‌گیرد.

برای الصاق هولوگرام به دستگاه مخصوص احتیاج است که با حرارت و فشار بالا به طور هم زمان روی سطح مورد نظر، فویل متال حاوی طرح هولوگرام را الصاق می‌کند و لایه حامل (پلی استر) از آن جدا می‌شود. فشار و دمای دستگاه حین الصاق به حدی است که فویل هولوگرام وارد بافت سطحی کاغذ می‌شود..

انهدام وامحاء اسناد

هرگاه به سندی نیاز نباشد بهترین اقدام حفاظتی انهدام آن است که باعث حفظ مفاد آن میشود. در صورت نیاز با امحاء وانهدام اسناد، کمیته تشخیص و تفکیک وامحاء اسناد تشکیل شده و بر اساس شرح وظایف، آیین نامه‌ها و دستورالعمل‌های موجود عملیات امحاء اسناد را انجام می‌دهند.

انهدام اسناد و اعضای کمیته امحا:

۱- نماینده حراست

۲- نماینده ریاست

۳- اقدام کننده

۴- بایگان

توجه: مشخصات مدارک مورد امحا در فرم شماره ۷ **حفاظتی** درج گردد.

برخی روش های متداول برای
انهدام اسناد:

الف: سوزاندن

ب: خورد کردن

پ: پودر کردن یا ریز ریز کردن

ت: خمیر کردن به کمک مواد شیمیایی

افشا:

افشاء یعنی عرضه مفاد اسناد و اطلاعات طبقه بندی شده بطور شفاهی و کتبی و یا هر طریقی که حفاظت و امنیت را از آن سلب و در اختیار افراد فاقد صلاحیت قرار گرفته باشد.

موارد مورد توجه در افشا اسناد طبقه بندی:

- ▶ 1- گزارش به موقع افشا توسط کارکنان
- ▶ 2- تحقیق و بازرسی اولیه روسا، مبنی بر افشا یا عدم افشا
- ▶ 3- گزارش به رده بالاتر و اقدامات اصلاحی
- ▶ 4- اعلام مراتب افشا به دارندگان سند، تقلیل طبقه بندی توسط صادر کننده سند
- ▶ 5- بررسی نحوه حفاظت سازمان، روشن شدن حقایق، تنبیه مقصرین، اقدامات اصلاحی توسط مدیران رده بالاتر.

مقامات مجاز برای تقلیل طبقه بندی:

- الف: مقام تعیین کننده اولیه
- ب: مقام جانشین یا بالاتر

روش تقلیل یا لغو طبقه بندی:

الف: بررسی مداوم یک سند و ارزیابی تغییرات آن.

ب: تقلیل طبقه بندی خود به خود.

پ: تغییر طبقه بندی پیش بینی شده. تقلیل بر اساس زمان بندی شامل: پرونده های امنیتی، تجهیزات رمز کننده و مراکز داده های الکترونیک نمی شود.

تقلیل طبقه بندی خود به خود:

اسناد گروه ۱: خیلی محرمانه پس از ۴ سال سری پس از ۷ سال بکلی سری

اسناد گروه ۲: عادی ۲ سال محرمانه ۲ سال خیلی محرمانه ۳ سال سری ۵ سال بکلی سری
اسناد گروه ۳: شامل اطلاعات واگذاری از سوی دولت های خارجی است و تقلیل طبقه بندی نمی شود.

اسناد گروه ۴: مطالب فوق لعاده حساس می باشد که ارزش آن به مرور زمان کاهش نمی یابد و تقلیل طبقه بندی نمی شود. و محدود به اسناد سری و به کلی سری است.

جعل چیست و جاعل به چه کسی اطلاق میشود؟

طبق قانون مجازات اسلامی، مجازات جعل احکام دادگاهها، مهر یا علامت شرکتها یا ادارت دولتی، اسکناس یا چک بانکی ۱ تا ۱۰ سال حبس، جعل مدارک تحصیلی ۱ تا ۳ سال حبس، جعل مهر یا علامت شرکت های غیردولتی ۳ ماه تا ۲ سال حبس است. و در صورتی که کارمندان یا مسوولان دولتی یا قضایی مرتکب جرم جعل شوند، مجازاتشان بیشتر از افراد عادی خواهد بود.

برخی قوانین افشا غیر مجاز اسناد طبقه بندی:

ماده ۲- هریک از کارکنان سازمانهای مذکور که حسب وظیفه مأمور حفظ اسناد سری و محرمانه دولتی بوده یا حسب وظیفه اسناد مذکور در اختیار او بوده و آنها را انتشار داده یا افشاء نماید یا به هر نحو دیگران را از مفاد آنها مطلع سازد در مورد اسناد سری به حبس جنایی درجه ۲ از دو تا ده سال و در مورد اسناد محرمانه به حبس از شش ماه تا سه سال محکوم می شود. در صورتی که افشای مفاد اسناد مذکور در اثر عدم رعایت نظامات یا در اثر غفلت و مسامحه حفاظت آنها صورت گرفته باشد، مجازات او سه ماه تا شش ماه حبس خواهد بود.

ماده ۳- هریک از کارکنان سازمان های مذکور یا اشخاص دیگر که اطلاعات یا مذاکرات یا تصمیمات سری و محرمانه دولتی را به نحوی از انحاء به کسی که صلاحیت اطلاع بر آن را ندارد بدهد یا موجبات افشاء یا انتشار آنها را فراهم نماید، عمل مرتکب در حکم افشاء یا انتشار اسناد سری یا محرمانه دولتی محسوب می شود

ماده ۵۰۱- هر کس نقشه ها یا اسرار یا اسناد و تصمیمات راجع به سیاست داخلی یا خارجی کشور را عالماً و عامداً در اختیار افرادی که صلاحیت دسترسی به آنها را ندارند قرار دهد یا از مفاد آن مطلع کند به نحوی که متضمن نوعی جاسوسی باشد، نظر به کیفیات و مراتب به یک تا ده سال حبس محکوم می شود.

ماده ۵۰۲- هر کس به نفع یک دولت بیگانه و به ضرر دولت بیگانه دیگر در قلمرو ایران مرتکب یکی از جرایم جاسوسی شود بنحوی که به امنیت ملی صدمه وارد نماید به یک تا پنج سال حبس محکوم خواهد شد.

ماده ۵۰۳- هر کس به قصد سرقت یا نقشه برداری یا کسب اطلاع از اسرار سیاسی یا نظامی یا امنیتی به مواضع مربوطه داخل شود و همچنین اشخاصی که بدون اجازه مأمورین یا مقامات ذیصلاح در حال نقشه برداری یا گرفتن فیلم یا عکسبرداری از استحکامات نظامی یا اماکن ممنوعه دستگیر شوند به شش ماه تا سه سال حبس محکوم می شوند.

معرفی فرم های مورد استفاده در حفاظت اماکن و اسناد

بطور کلی هشت نوع فرم در حفاظت مورد استفاده قرار می گیرد که جهت آشنایی با کاربرد آن ها، بشرح زیر معرفی می شوند.

فرم شماره (۱): گواهی خاتمه دسترسی به اطلاعات، اسناد و مدارک طبقه بندی شده:

این فرم جهت افرادی تکمیل می گردد که بنا به دلایلی از جمله انتقال، بازنشستگی، تغییر شغل، اخراج و غیره به دسترسی آنها خاتمه داده می شود.

فرم شماره (۲): ارقام رمز صندوق نسوز و اطلاعات مرتبط با آن:

این فرم برای هر صندوق مجهز به قفل رمز تکمیل و نزد مدیر آن قسمت نگهداری می گردد.

فرم شماره (۳): رسید نامه یا سند سری و بکلی سری: که قبلاً توضیح داده شد.

فرم شماره (۴): اطلاعات قسمت خارجی صندوق: قبلاً توضیح داده شد.

فرم شماره (۵): گواهی بازرسی و باز و بسته شدن صندوق های نسوز مجهز به قفل رمز: استفاده از این فرم، برای پیگیری موارد دسترسی های مجاز و هرگونه تبعات ناشی از آن بوده و اهمال بازرسان و مأمورین حفاظتی را براحتمی نشان می دهد.

فرم شماره ۱

((گواهی خاتمه دسترسی به اطلاعات و اسناد و مدارك طبقه بندی شده))

تاریخ

رتبه و سمت: نام و نام خانوادگی: نام پدر: قسمت:

اینجانب با مشخصات یاد شده بالا با آگاهی از مقررات و آیین نامه حفاظت اسناد و مدارك، اعلام می کنم که هیچ گونه سند یا مدارك طبقه بندی شده در اختیار من باقی نمانده و متعهد و ملزم می شوم که از این تاریخ اطلاعات طبقه بندی شده ای را که تا به امروز در دسترسی داشته ام، چه شفاهی و چه کتبی و یا به روش های دیگر در دسترس هیچ فرد یا سازمان غیرمجازی قرار ندهم و در صورت ارتکاب به چنین کردار خلافی، برابر قوانین دادرسی ی با من رفتار شود.

امضاء:

گواهی

بدین وسیله گواهی می کنم که نامبرده بالا در تاریخ تعهدنامه فوق را در حضور اینجانب خوانده و امضاء کرده است:

رتبه و سمت: نام و نام خانوادگی: قسمت:

فرم شماره ۲

ارقام رمز صندوق نسوز

طبقه بندی: فرم ترکیب ارقام رمز: تاریخ تنظیم:

ارقام رمز به رقم:

ارقام رمز به حروف:

قسمت استفاده کننده:

محل صندوق:

شماره صندوق:

مشخصات تغییر دهنده رمز:

تاریخ تغییر رمز:

مشخصات مسؤل صندوق:

رتبه و سمت: محل استفاده:

نام و نام خانوادگی: امضاء:

فرم شماره ۳

رسید نامه / سند

طبقه بندی سند:

بکلی سری: سری: شماره: تاریخ:

به:

از:

سندی که مشخصات آن در جدول ذیل قید شده ارسال می شود، خواهشمند است این رسید را امضاء کرده و اعاده فرمایند:

تاریخ نامه / سند: تعداد نسخ: موضوع: شماره:

نامه / سند: طبقه بندی نامه / سند:

تحویل گیرنده سند:

نام و نام خانوادگی: رتبه و سمت: تاریخ:

امضاء:

فرم شماره ۴

اطلاعات قسمت خارجی صندوق

قسمت: محل صندوق: شماره صندوق: تاریخ تغییر

رمز:

ملاحظات:

مشخصات اشخاصی که از رمز صندوق نسوز / قفسه آگاهی دارند:

ردیف	سمت	نام و نام خانوادگی	شماره صلاحیت	نشانی کامل منزل	تلفن
۱					
۲					

فرم شماره ۵

((گواهی بازرسی صندوق شماره ...))

نظریه بازرس مدیریت:

تاریخ، مشخصات و امضای بازرس مدیر:

نظریه بازرس حراست:

تاریخ، مشخصات و امضای بازرس حراست:

فرم شماره ۶

((گواهی بازرسی در خاتمه وقت اداری))

- ۱) کلیه صندوق ها، قفسه ها، کشوها، پنجره ها و قفل ها بسته است.
- ۲) اسناد و مدارك جمع آوری شده و هیچ گونه پرونده و مدارکی روی میزها وجود ندارد.
- ۳) کلیه چراغها و بخاری ها خاموش شده اند.
- ۴) ظروف اسناد باطله، خالی و کاربن های باطله نیز سوزانده شده اند.
- ۵) کلید اطاق ها، قفسه ها و کشوها در محل تعیین شده قرار دارند.
- ۶) مجدداً بازدید و هیچگونه وضع غیر عادی مشاهده نشد.

مشخصات بازرس حفاظتی

مسئول حفاظت اطاق

نام و نام خانوادگی

نام و نام خانوادگی

تاریخ

تاریخ

ساعت

ساعت

امضاء

امضاء

فرم شماره ۷

((فرم امحاء اسناد طبقه بندی شده))

شماره نامه / پرونده	نوع طبقه بندی نامه / پرونده	تعداد برگها	شرح مختصر	امحا براساس صورت جلسه مورد تصویب ... قرار گرفت

اسناد یاد شده بالا توسط کمیته امحاء (امضا کنندگان زیر) مورد رسیدگی و برگ شماری قرار گرفته و به روش ... امحاء شد.

اعضای کمیته: رتبه و سمت:

نام و نام خانوادگی:

(۱) نماینده صادرکننده سند:

(۲) نماینده حراست:

(۳) نماینده مدیریت:

فرم شماره ۸

نمونه دفتر ثبت اسناد سری و بکلی سری ارسالی و دریافتی

ردیف	شماره پرونده	قسمت	تعداد برگ	شرح مختصری از تجدید چاپ
	ذکر تاریخ ورود	صادرکننده گیرندگان		سند، تهیه رونوشت، بازدید، طبقه بندی

۱. در تاریخ از موجودی اسناد فوق بازدید به عمل آمد.

۲. در تاریخ از موجودی اسناد فوق بازدید به عمل آمد.

۳. در تاریخ از موجودی اسناد فوق بازدید به عمل آمد.

امضا:

نام و نام خانوادگی بازدید کننده:

موارد ذیل مورد توجه همکاران گرامی قرار گیرد :

- (۱) دفاتر و دبیرخانه های عادی مجاز به مفتوح نمودن و مطالعه نامه های طبقه بندی شده نمی باشند این قبیل نامه ها توسط دبیرخانه محرمانه که زیر نظر حراست می باشد باز شده و به سایر قسمت ها ارسال می گردد .
- (۲) در تمام مراحل گردش اسناد طبقه بندی شده در داخل ستاد و مراکز تابعه افراد غیر مجاز حق دسترسی یا استفاده از اسناد مزبور را ندارند .
- (۳) هرگونه تصویر برداری از اسناد و مکاتبات محرمانه و طبقه بندی شده بدون مجوز حراست اکیداً ممنوع می باشد.
- (۴) هرگونه ارجاع و نقل و انتقال اسناد طبقه بندی شده تنها پس از ثبت در دبیرخانه محرمانه انجام می گیرد .
- (۵) دبیرخانه محرمانه متولی نگهداری اسناد و سوابق از اولین مرحله آن یعنی تولید تا آخرین مرحله آن یعنی امحا می باشد.
- (۶) هیچ سندی یا نامه دارای طبقه بندی نایستی روی میز یا داخل کسوفهای بازنگهداری شود .
- (۷) در صورتی که سند به نام شخصی معین فرستاده شده است تسلیم آن به غیر از گیرنده اصلی غیر مجاز می باشد .
- (۸) اوراق باطله، پیش نویس، کاغذهای یادداشت که برای تهیه برنامه های طبقه بندی شده استفاده می شوند نیز باید به طور کامل نابود شوند . به طوریکه قابلیت بازسازی مجدد نداشته باشد و این امر تنها با حضور مسوول حراست سازمان و مراکز امکان پذیر می باشد .
- (۹) انتقال سند خیلی محرمانه و محرمانه به خارج از محیط کار ممنوع می باشد
- (۱۰) انتشار و افشاء اسناد محرمانه و انتقال آن به افراد غیر مجاز، ۶ ماه تا ۳ سال حبس به همراه خواهد داشت .
- (۱۱) هر یک از کارکنان که اطلاعات یا مذاکرات یا تصمیمات محرمانه را افشاء نمایند یا به افراد غیر مجاز منتقل نماید در حکم افشاء یا انتشار اسناد محرمانه دولتی محسوب می شود .