شناسایی و ارزش گذاری دارایی های IT

1) دسته بندی دارایی های فناوری اطلاعات

به تمام اطلاعات دیجیتال و غیر دیجیتال که توسط فرآیندهای کسب و کار ایجاد، پردازش، ذخیره، آرشیو و یا حذف می شوند دارایی اطلاعاتی گویند. مانند: رکوردهای دیتابیس، ایمیل ها، سورس کدها، اسناد کاغذی، طراحی ها، دیتابیس ها، داده های پردازش، عکس ها و ...

دارایی های اطلاعاتی یکی یا چند خصوصیت از سه خصوصیت زیر را دارا می باشند:

1) دارایی های اطلاعاتی بوسیله ارزش آنها در سازمان شناخته می شوند.
2) به راحتی با هزینه، مهارت، زمان، منابع یا ترکیبی از آن ها جایگزین نمی شوند.
3) بخشی از موجودیت های سازمان می باشند که بدون آن ها سازمان در معرض تهدید قرار می گیرد.

دارایی های اطلاعاتی از بعد محرمانگی به سه دسته تقسیم میگردند:

1-1) Confidential (محرمانه):

اگر این اطلاعات به بیرون نشت کند نتایج آن روی وجه سازمان و مسائل مالی تاثیرگذار است. مانند: قرداد مشتریان، جدول نرخ قیمت ها، اسناد فرآیند و نقشه محصولات جدید تولید شده.

1-2) Internal Use Only (تنها برای استفاده داخلی):

اگر این اطلاعات به بیرون از سازمان نشت کند نتایج آن منجر به ضرر و زیان مالی ناچیزی می شود. این اسناد آزادانه در اختیار کارمندان داخلی قرار می گیرند نظیر سیاست ها، اطلاعات آموزشی، بخشنامه ها.

1-3) Public (عمومی):

انتشار این اطلاعات هیچ ضرری برای سازمان ندارد. این اسناد باید توسط دپارتمان روابط عمومی یا فروش در اختیار عموم قرار گیرد. نظیر بروشورهای فروش و تبلیغاتی، مطالب مطبوعاتی.

2) شناسایی دارایی های فناوری اطلاعات:

دارایی های فناوری اطلاعات به سه دسته کلی اطلاعاتی، فیزیکی ، نیروی انسانی تقسیم می شوند که در جدول (الف) لیست تمامی دارایی ها دسته بندی و ارائه گردیده است.

Asset Category (دسته بندی دارایی ها)	Level 1 **(سطح 1)**	Level 2 **(سطح 2)**
1) **(Information Asset)** دارایی های اطلاعاتی	**1-1) Data**	**1-1-1) Personal**
		2-1-1) Financial
		3-1-1) Commercially Sensitive
		4-1-1) Safety Related
		5-1-1) Other Data Type
	2-1) End user service	**1-2-1) Electronic Mail**
		2-2-1) Application to Application Messaging
		3-2-1) Electronic Document Interchange
		4-2-1) Ad-hoc File Transfer
		5-2-1) Interactive Session
		6-2-1) Web Browsing
		7-2-1) Batch Processing
		8-2-1) Voice
		9-2-1) Video
		10-2-1) Other End User Service
	3-1) Software	**1-3-1) Funds Transfer**
		2-3-1) Financial
		3-3-1) Safety Critical
		4-3-1) Personal Information
		5-3-1) General
2) **(Physical Asset)** دارایی های فیزیکی	**1-2) Host**	**1-1-2) File Server**
		2-1-2) Database Server
		3-1-2) Application Server
		4-1-2) General Purpose Host
		5-1-2) Other Host
	2-2) Workstation	**1-2-2) Fixed Location Intelligent Workstation**
		2-2-2) Fixed Location Dumb Terminal
		3-2-2) Portable
		4-2-2) Personal Digital Assistant
		5-2-2) Other Workstation
	3-2) Storage Device	**1-3-2) Magnetic Disk Device**
		2-3-2) Magnetic Tape Device
		3-3-2) Optical Disk Device
		4-3-2) Other Storage Device
	4-2) Print Facilities	**1-4-2) Print Server**
		2-4-2) Printer
		3-4-2) Other Print Facilities
	5-2) Peripheral Devices	**1-5-2) Scanner**
		2-5-2) Fax Machines
		3-5-2) Other Peripheral Devices
		1-6-2) Bridge
		2-6-2) Router
		3-6-2) Hub/Repeater
		4-6-2) Layer 2 Switch
		5-6-2) Layer 3 Switch

Asset Category (دسته بندی دارایی ها)	Level 1 (سطح 1)	Level 2 (سطح 2)
	6-2) Network Distribution Component	6-6-2) Repeater
		7-6-2) Modem
		8-6-2) Multiplexor
		9-6-2) Network Termination Component
		10-6-2) ATM Switch Node
		11-6-2) X25 Switch Node
		12-6-2) Microwave Transceiver
		13-6-2) Infra-Red Transceiver
		14-6-2) Wireless Transceiver Access Point
		15-6-2) Laser Transceiver
		16-6-2) Ethernet/Gigabit Switch
		17-6-2) Satellite Ground Station
		18-6-2) VSAT Station
		19-6-2) PABX/PBX
		20-6-2) Automatic Call Distribution (ACD)
		21-6-2) Firewall/Security Gateway
		22-6-2) Message Translation Gateway
		23-6-2) Address Translation Gateway
		24-6-2) Protocol Converter
		25-6-2) Encryption Unit
		26-6-2) Universal Serial Bus (USB) Hub
		27-6-2) Other Network Distribution Component
	7-2) Network Management/Service Host	1-7-2) Directory Management System
		2-7-2) Message Store/Handling System
		3-7-2) Network User Authentication System
		4-7-2) Dial-up User Authentication System
		5-7-2) Firewall Management System
		6-7-2) Network Management System
		7-7-2) Encryption Management System
		8-7-2) TTP/CA/PKI Management System
		9-7-2) Other Network Management/Service
	8-2) Network Interface	1-8-2) Permanent Connection (PVC)
		2-8-2) Switched Connection (SVC)
		3-8-2) Wireless Connection
		4-8-2) Infra-Red Connection
		5-8-2) Laser Connection
		6-8-2) Microwave Connection
		7-8-2) Packet Radio Interface (GPRS)
		8-8-2) Other Network Interface
	9-2) Network Service	1-9-2) Data
		2-9-2) Voice
		3-9-2) Audio Video
	10-2) Communications Protocol	1-10-2) High Level Communications Protocol
		2-10-2) Low Level Communication Protocol
	11-2) Network Cabling	1-11-2) UTP (Unshielded twisted pair)
		2-11-2) STP (Shielded twisted pair)
		3-11-2) Coaxial
		4-11-2) Fiber
		5-11-2) Patch Panels
		6-11-2) Wiring Frames
		7-11-2) Termination Cabinets
	12-2) Telephony Devices	1-12-2) Telephony Handset
		2-12-2) Mobile Phone

Asset Category (دسته بندی دارایی ها)	Level 1 (سطح 1)	Level 2 (سطح 2)
		3-12-2) Other Telephony devices
	13-2) Media/Doc	1-13-2) Non Electronic
		2-13-2) Electronic
3) (Human Asset) دارایی های نیروی انسانی	1-3) Staff	1-1-3) Executives
		2-1-3) Managers
		3-1-3) Security Personnel
		4-1-3) Employees
		5-1-3) Field Personnel
	2-3) Temporary Workers	1-2-3) Front Office Worker
		2-2-3) Sensitive Position
	3-3) Contractors	1-3-3) Cleared Contractors
		2-3-3) Escorted Contractors
	4-3) Outsider	1-4-3) Contractors
		2-4-3) Temporary Worker
		3-4-3) Vendors
		4-4-3) Visitors

3) ارزش گذاری دارایی های فناوری اطلاعات:

برای ارزش گذاری دارایی ها می بایست ارزش دارایی های لیست شده با توجه به جدول الف از سه بعد محرمانگی، دسترس پذیری و صحت مورد بررسی قرار گیرند. که در ادامه نحوه ارزش گذاری دارایی ها به تفکیک ماهیت آنها بیان میگردد.

3-1) دارایی های اطلاعاتی:

3-1-1) محرمانگی دارایی های اطلاعاتی:

محرمانگی به معنای حفاظت از اطلاعات در برابر افشای غیر مجاز آن ها می باشد. ضربه حاصل از افشای اطلاعات می تواند منجر به خطر انداختن داده های حساس کارمندان شود.

جدول زیر به عنوان یک راهنما جهت شناسایی سطح محرمانگی به کار میرود.

سطح محرمانگی	توضیح
Low (کم)	اطلاعات غیر حساس که می تواند در دسترس عموم قرار گیرد. ضربه حاصل از افشای غیر مجاز آن ها نباید به سازمان ضرر وارد کند. نظیر: مطلب مطبوعاتی، روزنامه شرکت، اطلاعات روی وب سایت شرکت.
Medium (متوسط)	اطلاعاتی که نباید بیرون از سازمان و بخش های خارجی قرار گیرد. افشای غیر مجاز این اطلاعات می تواند ضرر کمی به سازمان متحمل کند. مثل چارت سازمانی، خطوط تلفن داخلی .
High (زیاد)	اطلاعات خیلی حساس و محرمانه با ارزش بالا که توسط افراد خاص مورد استفاده قرار می گیرند. افشای غیر مجاز آن ها ممکن است چندین ضرر داشته باشد. نظیر: بدهی مالی یا حقوقی، ضرر رقابتی و کاهش برند اطلاعات قیمت سرویس گیرنده ها، استراتژی های

تجاری.

3-1-2) صحت دارایی های اطلاعاتی:

صحت به دو مقوله کامل بودن و دقیق بودن اطلاعات بر می گردد. با تغییرات غیر مجاز صحت کاهش می یابد. اگر صحت داده ها قابل برگشت نباشد استفاده از داده های آلوده منجر به بروز عدم دقت، تفکیک و یا اشتباهات تقسیم گیری می شود.

جدول زیر به عنوان یک راهنما جهت شناسایی سطح صحت اطلاعات به کار می رود.

سطح صحت	توضیح
Low (کم)	اگر دو مقوله کامل بودن و دقیق بودن اطلاعات کاهش یابد حداقل ضربه را به کسب و کار وارد می کند.
Medium (متوسط)	اگر دو مقوله کامل بودن و دقیق بودن اطلاعات کاهش یابد حداقل ضربه قابل توجه به کسب و کار وارد می کند.
High (زیاد)	تنزل صحت اطلاعات غیر قابل پذیرش است.

3-1-3) دسترس پذیری دارایی های اطلاعاتی:

دسترس پذیری نشان می دهد که اطلاعات مورد نیاز در زمان از دست دادن، تا چه حد سریعا در اختیار قرار می گیرد.

اگر اطلاعات حساس برای کاربران نهایی قابل دسترس نباشند ممکن است ماموریت کسب و کار تحت تاثیر قرار گیرد.

جدول زیر به عنوان راهنمایی برای سطح دسترس پذیری اطلاعات ارائه می گردد.

سطح دسترس پذیری	توضیح
Low (کم)	اگر دارایی های اطلاعاتی تا 7 روز در دسترس نباشد. حداقل ضربه را برای سازمان دارد.
Medium (متوسط)	اگر دارایی های اطلاعاتی تا 48 ساعت در دسترس نباشد. ضربه قابل توجهی به سازمان وارد می شود.
High (زیاد)	دارایی های اطلاعاتی بصورت 24 ×7 مورد نیاز هستند.

3-2) دارایی نیروی انسانی:

از آنجایی که اطلاعات در راستای نیازهای کسب و کار توسط نیروهای درون سازمانی و بیرون سازمانی مورد دسترسی و به کار گرفته می شوند ضروری است که شناسایی شود چه افرادی از درون سازمان یا بیرون سازمان به دارایی های اطلاعاتی سازمان ها دسترسی دارند و از آن ها استفاده می کنند.

آنالیز نیروی انسانی ای که حق دسترسی به دارایی های سازمان را دارند می بایست بوسیله مالک فرآیندهای سازمان یا مسئول دستورالعمل ها و فرآیندها صورت گیرد.

3-2-1) مسئولیت:

	Responsible	Accountable	Consulted	Informed
شناسایی و ارزش گذاری دارایی ها	_	_	_	کمیته عالی

3-2-2) ارزش گذاری:

دارایی نیروی انسانی باید شامل نقش هایی (Role) که توسط کارمندان، کارمندان قراردادی، پیمانکاران و نیروهای آن ها مورد استفاده قرار می گیرند شود.

3-2-2-1) سطح محرمانگی:

جدول زیر یک راهنما برای شناسایی سطح محرمانگی و نحوه دسته بندی ارائه می نماید.

سطح محرمانگی	توضیحات
Low (کم)	نقش یا شخص ثالثی که دسترسی محدودی به دسته "عمومی" دارایی های سازمان دارد. نقض امنیتی توسط فردی که نقش به آن واگذار شده تاثیر ناچیزی روی عملیات سازمان می گذارد.
Medium (متوسط)	نقش یا شخص ثالثی که دسترسی محدودی به دارایی های دسته "عمومی" و "داخلی" سازمان دارد. نقض امنیتی توسط فردی که نقش به آن واگذار شده تاثیر ملایمی روی عملیات سازمان می گذارد.
High (زیاد)	نقش کارمند یا شخص ثالثی که دسترسی محدودی به همه انواع دارایی های اطلاعاتی شامل دسته محرمانه یا دارایی های سازمان دارد. نقض امنیتی توسط فردی که نقش به آن واگذار شده به شدت روی عملیات سازمان تاثیر دارد.

3-2-2-2) سطح صحت دارایی:

این جدول یک راهنما برای شناسایی سطح صحت و دسته بندی آن ها است.

سطح صحت	توضیحات
Low (کم)	نقش یا شخص ثالثی که دسترسی محدود به تغییر دارایی های اطلاعاتی از دسته "عمومی" و "داخلی" دارد و کارش مورد نظارت قرار می گیرد. نقض امنیتی توسط شخصی که نقش به آن واگذار شده است تاثیر ناچیزی روی عملیات سازمان دارد.

Medium (متوسط)	نقش یا شخص ثالثی که دسترسی به تغییر دارایی های اطلاعاتی از دسته "داخلی" و "عمومی" دارد. نقض امنیت توسط شخصی که نقش به آن واگذار شده است تاثیر ملایمی روی عملیات سازمان دارد.
High (زیاد)	نقش یا شخص ثالثی که دسترسی به تغییر دارایی های اطلاعاتی از دسته "محرمانه" را دارد یا امکان تغییر پیکربندی دارایی های حیاتی IT را دارد. نقض امنیت توسط شخصی که نقش به آن واگذار شده است به شدت روی عملیات سازمان تاثیر می گذارد.

3-2-2-3) سطح دسترس پذیری:

این جدول یک راهنما برای شناسایی سطح دسترس پذیری و دسته بندی آن ها است.

سطح دسترس پذیری	توضیحات
Low (کم)	عدم دسترسی به شخصی که ثالثی که نقش به آن واگذار شده است تاثیر ناچیزی روی عملیات سازمان دارد.
Medium (متوسط)	عدم دسترسی به شخصی که ثالثی که نقش به آن واگذار شده است تاثیر ملایمی روی عملیات سازمان دارد.
High (زیاد)	عدم دسترسی به شخصی که ثالثی که نقش به آن واگذار شده است به شدت روی عملیات سازمان تاثیر دارد.

3-3) دارایی های فیزیکی (غیر اطلاعاتی)

داده ها بوسیله تکنولوژی هایی مورد پردازش قرار می گیرند. دارایی هایی که در ایجاد، پردازش، تولید خروجی ها و ذخیره سازی استفاده میشوند نیازمند شناسایی و ارزش گذاری.

ارزش گذاری دارایی های غیر اطلاعاتی باید الزامات محرمانگی، صحت و دسترس پذیری کسب و کار و فرآیندهای آن که در آن ها استفاده می شود را به حساب آورد. این الزامات باید دارایی های حیاتی کسب و کار و فرآیندهای آن را تعیین کنند و در تعریف طرح از سرگیری کسب و کار یا طرح بازیابی بحران استفاده شوند. این محاسبات باید یکسان در مورد دارایی ها صورت گیرند.

3-3-1) سطح محرمانگی :

فاکتور محرمانگی بوسیله سرویسی که توسط دارایی خاصی در فرآیند کسب و کار که الزامات محرمانگی اطلاعات، داده ها ذخیره شده و پردازش شده را دارد تعیین خواهد شد.

جدول زیر نحوه شناسایی الزامات محرمانگی و نحوه دسته بندی آن ها ارائه می دهد.

الزامات محرمانگی	توضیحات

Low (کم)	اطلاعاتی که توسط دارایی مورد پردازش، ذخیره سازی یا جا به جایی قرار می گیرد یا سرویسی که توسط دارایی ارائه می شود در فرآیند سازمانی الزام محرمانگی پایینی دارد.
Medium (متوسط)	اطلاعاتی که توسط دارایی مورد پردازش، ذخیره سازی یا جا به جایی قرار می گیرد یا سرویسی که توسط دارایی ارائه می شود در فرآیند سازمانی الزام محرمانگی متوسطی دارد.
High (زیاد)	اطلاعاتی که توسط دارایی مورد پردازش، ذخیره سازی یا جا به جایی قرار می گیرد یا سرویسی که توسط دارایی ارائه می شود در فرآیند سازمانی الزام محرمانگی بالایی دارد.

3-3-2) سطح صحت :

فاکتور صحت باید بوسیله قابلیت اطمینان و اعتماد به دارایی خاصی از فرآیند تجاری خاص با الزامات صحت تعیین شود.

جدول زیر نحوه شناسایی الزام صحت و نحوه دسته بندی آن ها ارائه می دهد.

الزامات صحت	توضیحات
Low (کم)	قابلیت اطمینان و اعتماد سرویسی که بوسیله دارایی خاصی در فرآیند سازمانی ارائه می شود کم است. اطلاعات پردازشی، ذخیره سازی یا جا به جایی یا سرویس ارائه شده توسط دارایی در فرآیند سازمانی الزام صحت کمی دارد.
Medium (متوسط)	قابلیت اطمینان و اعتماد سرویسی که بوسیله دارایی خاصی در فرآیند سازمانی ارائه می شود متوسط است. اطلاعات پردازشی، ذخیره سازی یا جا به جایی یا سرویس ارائه شده توسط دارایی در فرآیند سازمانی الزام صحت متوسطی دارد.
High (زیاد)	قابلیت اطمینان و اعتماد سرویسی که بوسیله دارایی خاصی در فرآیند سازمانی ارائه می شود بالا است. اطلاعات پردازشی، ذخیره سازی یا جا به جایی یا سرویس ارائه شده توسط دارایی در فرآیند سازمانی الزام صحت بالایی دارد.

3-3-3) سطح دسترس پذیری :

معیار دسترس پذیری برمبنای ضربه ناشی از عدم دسترس پذیری به دارایی بر روی فرآیند سازمانی تعیین خواهد شد.

جدول زیر نحوه شناسایی الزام دسترس پذیری و دسته بندی آن ها ارائه می دهد.

الزامات دسترس پذیری	توضیحات
Low (کم)	ضربه ناشی از عدم دسترسی به دارایی از فرآیند سازمانی کم است. اطلاعات مورد پردازش/ ذخیره شده/ در حال جا به جایی، یا سرویس های ارائه شده توسط دارایی در فرآیند سازمانی الزام دسترس پذیری کمی دارد.
Medium (متوسط)	ضربه ناشی از عدم دسترسی به دارایی از فرآیند سازمانی متوسط است. اطلاعات مورد پردازش/ ذخیره شده/ در حال جا به جایی یا سرویس های ارائه شده توسط دارایی در

	فرآیند سازمانی الزام دسترس پذیری متوسطی دارد.
High (زیاد)	ضربه ناشی از عدم دسترسی به دارایی از فرآیند سازمانی زیاد است. اطلاعات مورد پردازش/ ذخیره شده/ در حال جا به جایی یا سرویس های ارائه شده توسط دارایی در فرآیند سازمانی الزام دسترس پذیری زیادی دارد.

4) تعیین سطح حساسیت دارایی ها:

ارزش دارایی	وضعیت حساسیت	توضیح
8-9	خیلی حساس	فقدان یا در معرض خطر قرار گرفتن الزامات CIA منجر به زیان تجاری یا ضربه شدید در تجارت می شود. سیستم هایی که اطلاعات محرمانه را نگهداری می کنند یا دارایی های اطلاعاتی با ارزش 8و9
6-7	حساس	فقدان یا در معرض خطر قرار گرفتن الزامات CIA منجر به زیان به فرآیند تجاری یا ضربه شدید تنها روی فرآیند تجاری می شود. سیستم هایی که اطلاعات محرمانه یا دارایی اطلاعاتی با ارزش 6و7 نگهداری می کنند .
5	حساسیت ملایم	فقدان یا در معرض خطر قرار گرفتن الزامات CIA منجر به زیان به فرآیند تجاری یا ضربه شدید تنها روی فرآیند تجاری می شود. سیستم هایی که اطلاعات محرمانه یا دارایی اطلاعاتی با ارزش 6و7 نگهداری می کنند .
4-3	غیر حساس	همه سیستم های دیگر که در هیچکدام از دسته های بالا قرار نمی گیرند.