Sample Termination Checklist

Employee Name

Group or Business Unit

Manager / Supervisor Name

Primary User ID

Termination Date / Time

Reviewed by Security Officer (CSO/ISO) (Date / Time)

HIGH = 1 hour
MED = Same Day
LOW = 48 hours

				Had Access		Disabled / Received				Removed Entitlements?				Updated Vendor Contact Info?				Review Performed By		
#	Item	System Name	Risk Level	Yes	No	Yes	N/A	Status	User ID	Yes	No	N/A	Status	Yes	No	N/A	Status	Person	Date / Time	SLA Met?
	*Note: This section is designed to mitigate immediate risk, and certain items may be repeated in other sections. This is a checklist for HR and IT to follow **during** the exit process.*																			
1	**Disable Major Logical Access Upon Termination**																			-
1.1	Central Identity / Primary Identity	XYZ.com domain	HIGH					-	*				RISK				RISK			-
1.2	VPN Access	VPN	HIGH					-	*				RISK				RISK			-
1.3	Disable remote access to voicemail	Telecom	HIGH																	
2	**Recover Company Assets, Access, and Equipment upon Termination**																			-
2.1	Laptop	Company-owned Asset	HIGH					-					RISK				RISK			-
2.2	Corporate Card	Financial Control	HIGH					-					RISK				RISK			-
2.3	Cell Phone	Company-owned Asset	HIGH					-					RISK				RISK			-
2.4	ID Badge	Access Control	HIGH					-					RISK				RISK			-
2.5	Electronic Badge (if not the same as the ID badge)	Access Control	HIGH					-					RISK				RISK			-
2.6	Office Keys	Access Control	MED					-					RISK				RISK			-
2.7	Offsite Storage Keys	Access Control	HIGH					-					RISK				RISK			-
2.8	Bin / Desk / File Drawer Keys	Access Control	LOW					-					RISK				RISK			-
2.9	VPN token	Access Control	HIGH					-					RISK				RISK			-
2.10	Parking Pass	Access Control	LOW					-					RISK				RISK			-
3	**Redirect Company Contact Information**																			
3.1	Forward e-mail to Manager	E-mail	HIGH																	
3.2	Forward cell phone number to Manager	Telecom	HIGH																	
3.3	Forward desk phone number to Manager	Telecom	HIGH																	
3.4	Forward instant messenger to Manager	Instant Messenger	HIGH																	
3.5	Forward fax number to Manager	Telecom	HIGH																	
	*Note: The following sections are designed as a comprehensive checklist, to be executed **subsequent** to the exit process.*																			
4	**Ship Home Office Equipment**																			-
4.1	Monitor	Company-owned Asset	LOW					-					RISK				RISK			-
4.2	Docking Station	Company-owned Asset	LOW					-					RISK				RISK			-
4.3	VoIP Phone	Company-owned Asset	LOW					-					RISK				RISK			-
4.4	Router	Company-owned Asset	LOW					-					RISK				RISK			-
4.5	Printer	Company-owned Asset	LOW					-					RISK				RISK			-
5	**Physical Access**																			-
5.1	Building keys	Physical Access	HIGH					-					RISK				RISK			-
5.2	Office Keys	Physical Access	MED					-					RISK				RISK			-
5.3	Master keys	Physical Access	HIGH					-					RISK				RISK			-
6	**Storage**																			-
6.1	Safe keys	Storage Access	MED					-					RISK				RISK			-
6.2	Safe combinations (Disclose)	Storage Access	HIGH					-					RISK				RISK			-
6.3	Safe combinations – Changed	Storage Access	MED					-					RISK				RISK			-
6.4	Filing cabinet / desk / bin keys	Storage Access	LOW					-					RISK				RISK			-
6.5	Keys to shared filing areas	Storage Access	LOW					-					RISK				RISK			-
6.6	Combinations to locked, shared filing areas – Changed	Storage Access	LOW					-					RISK				RISK			-
6.7	Keys to offsite storage	Storage Access	HIGH					-					RISK				RISK			-
6.8	Combinations to locked, offsite storage- Changed	Storage Access	HIGH					-					RISK				RISK			-
6.9	Safe Deposit boxes – Revoke Access, Update Vendor Contact	Storage Access	HIGH					-					RISK				RISK			-
6.10	Keys to Safe Deposit boxes	Storage Access	HIGH					-					RISK				RISK			-
7	**Electronic Access**																			-
7.1	PINs – Deny / Disable	Physical Access	HIGH					-					RISK				RISK			-
7.2	Obtain Badges	Physical Access	HIGH					-					RISK				RISK			-
7.3	Badges – disabled	Physical Access	LOW					-					RISK				RISK			-
7.4	Biometrics – Retina – Deny / Disable	Physical Access	MED					-					RISK				RISK			-
7.5	Biometrics - Finger prints – Deny / Disable	Physical Access	MED					-					RISK				RISK			-
7.6	Biometrics - Palm signatures – Deny / Disable	Physical Access	MED					-					RISK				RISK			-
7.7	Biometrics - Facial recognition – Deny / Disable	Physical Access	MED					-					RISK				RISK			-
7.8	Obtain Fobs / tokens	Physical Access	HIGH					-					RISK				RISK			-
7.9	Fobs / tokens – Disabled	Physical Access	LOW					-					RISK				RISK			-
7.10	Electronic safe PINs (Disclose)	Physical Access	HIGH					-					RISK				RISK			-
7.11	Electronic safe PINs – Changed	Physical Access	MED					-					RISK				RISK			-
7.12	Alarm System – PINs / Biometrics – Deny / Disable	Honeywhirl	HIGH					-					RISK				RISK			-
7.13	Alarm System – Common codes changed	Honeywhirl	HIGH					-					RISK				RISK			-
8	**Hosting – Vendors**																			-
8.1	Domain Registrar	ABC Hosting	HIGH					-					RISK				RISK			-
8.2	DNS Provider	ABC Hosting	HIGH					-					RISK				RISK			-
8.3	Certificate / Trust provider	Symantesign	HIGH					-					RISK				RISK			-
8.4	Hosting provider	ABC Hosting	HIGH					-					RISK				RISK			-
8.5	Cloud vendor	ABC Hosting	HIGH					-					RISK				RISK			-

8.6	FTP / File sharing	XYZ Hosting	HIGH		-		RISK		RISK		-
8.7	Web Conferencing – Disable user account, Update Vendor Contact	Webulex	MED		-		RISK		RISK		-
8.8	Web Conferencing – Disable "unattended" access	Webulex	HIGH		-		RISK		RISK		-
8.9	Instant Messenger	Groogle	HIGH								-
8.10	Hosted Fax Service	eFlax	MED								-
9	**Financial Access and Controls – Vendors**										-
9.1	**Bank access – Revoke, Change authentication credentials**										-
9.2.1		Bank A – Account 1 – Payroll	HIGH		-		RISK		RISK		-
9.2.2		Bank A – Account 2 – Operations	HIGH		-		RISK		RISK		-
9.2.3		Bank B – Credit Card	HIGH		-		RISK		RISK		-
9.2.4		Bank C – Capital Savings	HIGH		-		RISK		RISK		-
9.3	Payroll vendor – Revoke Employee (review) access	Surideon	MED		-		RISK		RISK		-
9.4	Payroll vendor – Revoke Administrative access	Surideon	HIGH		-		RISK		RISK		-
9.5	Cloud-based ERP – Remove regular user access	Microswift Blue	MED		-		RISK		RISK		-
9.6	Cloud-based ERP – Remove administrative access	Microswift Blue	HIGH		-		RISK		RISK		-
9.7	Travel Portal – Disable user access	Travacceleration	MED		-		RISK		RISK		-
9.8	Travel Portal – Disable administrative access	Travacceleration	HIGH		-		RISK		RISK		-
9.9	Obtain Corporate Card	Bank B	HIGH		-		RISK		RISK		-
9.10	Disable Corporate Card	Bank B	MED		-		RISK		RISK		-
9.11	**Supplier purchasing accounts – Disable, Update Vendor Contact**										-
9.12.1		Office Train Station	HIGH		-		RISK		RISK		-
9.12.2		PC's R Us	HIGH		-		RISK		RISK		-
9.12.3		Servers R Us	HIGH		-		RISK		RISK		-
9.12.4		AccuHardware switches & routers	HIGH		-		RISK		RISK		-
10	**Data and Telecommunications - Vendors**										
10.1	Private Circuit (WAN) – Revoke Access, Update Vendor Contact										
10.2.1		AT&P MPLS	HIGH		-		RISK		RISK		-
10.2.2		Verizoom MPLS	HIGH		-		RISK		RISK		-
10.3	Internet Circuit (ISP) – Revoke Access, Update Vendor Contact										
10.4.1		Cogulent (Main Office)	HIGH		-		RISK		RISK		-
10.4.2		Comcrash (Branch Access)	HIGH		-		RISK		RISK		-
10.5	Telecom – Local Provider – Revoke Access, Update Vendor Contact	Pacific Ding	HIGH		-		RISK		RISK		-
10.6	Telecom – Long Distance Provider – Revoke Access, Update Vendor Contact	AT&P	HIGH		-		RISK		RISK		-
10.7	PBX (Phone system) Vendor and Maintenance – Revoke access, Update Vendo	AAA Telecom	HIGH		-		RISK		RISK		-
10.8	Cloud VoIP / Conferencing – Revoke Access, Update Contact Information	Meet-Us	HIGH		-		RISK		RISK		-
10.9	Cloud VoIP Vendor – Revoke Access, Update Contact Information	Squipe	HIGH		-		RISK		RISK		-
10.10	Audio Conferencing – Disable personal conference bridge line	Megaconference	HIGH		-		RISK		RISK		-
10.11	Audio Conferencing – Revoke Access, Update Contact Information	Megaconference	HIGH		-		RISK		RISK		-
10.12	Audio Conferencing – Update bridge line for recurring meetings	Megaconference	HIGH		-		RISK		RISK		-
11	**Remote Access**										
11.1	VPN Access – Disable	Crisco	HIGH		-		RISK		RISK		-
11.2	VPN Access – Revoke token / certificate	Veriswine	HIGH		-		RISK		RISK		-
11.3	VPN Access – Remove biometric signatures or set to “deny”	Biotech	HIGH		-		RISK		RISK		-
11.4	Modem Access – Disable	RAS	HIGH		-		RISK		RISK		-
11.5	Serial Line / Terminal access – Disable	RAS	HIGH		-		RISK		RISK		-
11.6	Managed VPN – Disable access, Update vendor contact	Verizoom	HIGH		-		RISK		RISK		-
12	**Internet-facing Applications (Internally-hosted)**										
12.1	E-mail	SwellMail	HIGH		-		RISK		RISK		-
12.2	Sharepoint or E-Room	Sharepoint	HIGH		-		RISK		RISK		-
12.3	FTP / File sharing	Mover-THEM	HIGH		-		RISK		RISK		-
12.4	ERP (time sheets, expense reports)	PeopleSwift	HIGH		-		RISK		RISK		-
12.5	Corporate Intranet / Portal	PeopleSwift-Portal	HIGH		-		RISK		RISK		-
12.6	CRM	Remediary	HIGH		-		RISK		RISK		-
12.7	Support website	SupportSite	HIGH		-		RISK		RISK		-
12.8	Corporate Instant Messaging	Lynky	HIGH		-		RISK		RISK		-
13	**Forward or Disable Contact Information**										
13.1	E-mail										
13.1.1	--Disable e-mail or Forward to Manager	SwellMail	HIGH		-		RISK		RISK		-
13.1.2	--Provide Manager access to e-mail (mailbox and archives)	SwellMail	LOW		-		RISK		RISK		-
13.2	Cell Phone										
13.2.1	--Disable cell phone or Forward number to Manager	Verizoom	HIGH		-		RISK		RISK		-
13.2.2	--Change cell phone voicemail password	Verizoom	HIGH		-		RISK		RISK		-
13.2.3	--Provide Manager access to cell phone voice mail, or delete	Verizoom	LOW		-		RISK		RISK		-
13.3	Desk Phone / Soft Phone										
13.3.1	--Disable IP PBX (Soft Phone) Access	PhoneBox	HIGH		-		RISK		RISK		-
13.3.2	--Forward phone number to Manager or Disable	PhoneBox	HIGH		-		RISK		RISK		-
13.3.3	--Change voicemail password	PhoneBox	HIGH		-		RISK		RISK		-
13.3.4	--Provide Manager access to voicemail or delete	PhoneBox	LOW		-		RISK		RISK		-
13.4	Instant Messenger										
13.4.1	--Disable Instant Messenger access or change password	Lynky	HIGH		-		RISK		RISK		-
13.4.2	--Provide Instant Messenger access to Manager	Lynky	HIGH		-		RISK		RISK		-
13.5	Fax										
13.5.1	--Disable fax number or forward to Manager	eFlax	HIGH		-		RISK		RISK		-
13.5.2	--Disable access to Fax mailbox or change password	eFlax	HIGH		-		RISK		RISK		-
13.5.3	--Provide access to Fax mailbox to Manager	eFlax	LOW		-		RISK		RISK		-
14	**Control Systems / Task-specific Servers (Assumes network access required)**										
14.1	Power control	Physical Systems	LOW		-		RISK		RISK		-

14.2	UPS Systems	Physical Systems	LOW					-					RISK				RISK			-
14.3	Air handlers / chillers / AC	Physical Systems	LOW					-					RISK				RISK			-
14.4	Telecom / datacom (Managed termination endpoint)	Physical Systems	LOW					-					RISK				RISK			-
14.5	Door Locks	Physical Systems	LOW					-					RISK				RISK			-
14.6	Alarm Systems	Physical Systems	LOW					-					RISK				RISK			-
14.7	Camera Systems	Physical Systems	LOW					-					RISK				RISK			-
14.8	SCADA Servers	Fountain Pump	LOW					-					RISK				RISK			-
14.9	Task Servers	JobServer1	LOW					-					RISK				RISK			-
14.10	Controller Servers	Elevator Controller	LOW					-					RISK				RISK			-
14.11	Tape / Media Controllers	Backup1	LOW					-					RISK				RISK			-
14.12	PBX (Phone System)	PhoneBox	LOW					-					RISK				RISK			-
14.13	Time Clock System	TickTock	LOW					-					RISK				RISK			-
15	**Infrastructure Devices**																			
15.1	Internet Router																			
15.1.1	--Change passwords for well-known accounts	INETRTR01	HIGH					-					RISK				RISK			-
15.1.2	--Remove local access	INETRTR01	HIGH					-					RISK				RISK			-
15.2	Firewalls – Review / Remove access																			
15.2		DFWFW	HIGH					-					RISK				RISK			-
15.2		ATLFW	HIGH					-					RISK				RISK			-
15.3	Routers – Review / Remove access																			
15.3		DFWRTR	LOW					-					RISK				RISK			-
15.3		ATLRTR	LOW					-					RISK				RISK			-
15.4	Switches – Review / Remove access																			
15.4	--DFW, 5th Floor	DFWSW05-01	LOW					-					RISK				RISK			-
15.4	--DFW, 6th Floor	DFWSW06-01	LOW					-					RISK				RISK			-
15.4	--ATL, 2nd Floor	ATLSW02-01	LOW					-					RISK				RISK			-
15.4	--DFW DMZ	DFWSWDMZ	HIGH					-					RISK				RISK			-
15.4	--ATL DMZ	ATLSWDMZ	HIGH					-					RISK				RISK			-
15.5	Intrusion Detection / Prevention Systems – Review / Remove access	SourceFlare	LOW					-					RISK				RISK			-
15.6	Network Tap / Bypass – Review / Remove access	Bypass	LOW					-					RISK				RISK			-
15.7	Application Deliery Controller	F55	LOW					-					RISK				RISK			-
16	**Servers and Applications**																			
16.1	Central Directory User Object / Primary Identity	*(List of all domains)*																		
16.1.1	*--(Back up, Disable, Remove Access)*	DOMAIN1.PVT	HIGH					-					RISK				RISK			-
16.1.2	*--(Back up, Disable, Remove Access)*	DEVDOMAIN.PVT	LOW					-					RISK				RISK			-
16.2	Servers – Audit all servers that leverage local users	*(List of all servers)*																		
16.2.1	*--(Document, Disable, Remove Access)*	DFWSRV01	HIGH					-					RISK				RISK			-
16.2.2	*--(Document, Disable, Remove Access)*	DFWAPP01	LOW					-					RISK				RISK			-
16.2.3	*--(Document, Disable, Remove Access)*	DFWSERVER	LOW					-					RISK				RISK			-
16.2.4	*--(Document, Disable, Remove Access)*	MAIL1	LOW					-					RISK				RISK			-
16.2.5	*--(Document, Disable, Remove Access)*	DFWDATABASE	LOW					-					RISK				RISK			-
16.2.6	*--(Document, Disable, Remove Access)*	ATLFILE01	LOW					-					RISK				RISK			-
16.2.7	*--(Document, Disable, Remove Access)*	ATLSHAREPOINT	LOW					-					RISK				RISK			-
16.2.8	*--(Document, Disable, Remove Access)*	ATLAPP01	LOW					-					RISK				RISK			-
16.2.9	*--(Document, Disable, Remove Access)*	WEB1	LOW					-					RISK				RISK			-
16.2.10	*--(Document, Disable, Remove Access)*	DFWWEB02	LOW					-					RISK				RISK			-
16.3	Databases – Audit all database instances that leverage local permissions	*(List of databases or instances)*																		
16.3.1	*--(Document, Disable database user, Remove Database access)*	DFWDATABASE/intranet	MED					-					RISK				RISK			-
16.3.2	*--(Document, Disable database user, Remove Database access)*	DFWDATABASE/accounting	MED					-					RISK				RISK			-
16.3.3	*--(Document, Disable database user, Remove Database access)*	DFWDATABASE/hcmapp	MED					-					RISK				RISK			-
16.3.4	*--(Document, Disable database user, Remove Database access)*	ATLSHAREPOINT/sharepoint	MED					-					RISK				RISK			-
16.3.5	*--(Document, Disable database user, Remove Database access)*	MAIL1/maildb	MED					-					RISK				RISK			-
16.4	Internal Applications – Audit all applications that use local authentication	*(List of internal applications)*																		
16.4.1	*--(Document, Disable application user, Remove Application access)*	CVS / Git	HIGH					-					RISK				RISK			-
16.4.2	*--(Document, Disable application user, Remove Application access)*	PeopleSwift-Accounting	HIGH					-					RISK				RISK			-
16.4.3	*--(Document, Disable application user, Remove Application access)*	PeopleSwift-HCM	HIGH					-					RISK				RISK			-