

ISO 27001 information security policies and classification checklist

Objectives:	Procedures	Status	Notes
Information classification	Describes how information should be classified. Include a data ownership policy and a data treatment table.		
Data protection	Covers data protection: How the company will manage personal data and precautions employees should take to avoid infringing on others rights.		
Host access controls	Describes the:		
	Logon process		
	Login banners		
	Password rules		
	Audit rules		
	Data roles		
Internet usage	Describes acceptable "Netiquette."		
E-mail usage	Warns users about the dangers of email.		
Virus control	Describes the rules for virus protection and tells users what to do if their computers are infected.		
Backup and data disposal	The backup policy mandates that systems should be backed up when they are in use and that these backups should be tested and protected according to the needs of the business. The disposal policy will mandate that:		
	Disks should be destroyed before disposal.		
	CDs should be sanded and snapped.		
	Tapes should be degaussed.		
Remote access	How to access the network remotely.		
Physical protection	Describes physical protection.		
Encryption	Describes confidentiality.		
Software licensing	Describes use of legal software.		
Acceptable use policy (AUP)	This document is a little different from the rest because it should be educational in its nature. It exemplifies acceptable use of company facilities and IT equipment and describes forbidden activities. Banned behavior tends to include:		
	Using illegal software		
	Viewing offensive material		
	Hacking or virus distribution or otherwise infringing on an individual's rights The big question here is whether to allow or disallow personal use; the latter is becoming increasingly difficult in some legal jurisdictions.		