



## Recruitment screening

Applications for employment should be screened if the job involves access to IT facilities handling sensitive information.

The following checks should be made on all such applications:

1. at least two satisfactory character references, one business and one personal;
2. a check (for completeness and accuracy) of the applicant's curriculum vitae;
3. confirmation of academic and professional qualifications;
4. an identification check, e.g. passport;
5. a credit check for employment in particularly sensitive jobs, e.g. control of finance.

## Confidentiality agreement

Users of organisational IT facilities should sign an appropriate confidentiality (non-disclosure) undertaking. Employees should normally sign such an undertaking as part of their initial conditions of employment.

Agency staff and third party users not already covered by an existing contract (containing the confidentiality undertaking) should be required to sign a confidentiality agreement prior to connection to organisational IT facilities.

Confidentiality agreements should be reviewed when there are changes to terms of employment or contract, particularly when employees are due to leave the organisation, or contracts due to end.

## Disciplinary process

There should be a formal disciplinary process for employees who have allegedly violated organisational security policies and procedures. Such a process will act as a deterrent to employees who might be inclined to disregard security procedures. Additionally, it should ensure correct, fair treatment for employees who are suspected of committing serious or persistent breaches of security.

## Personnel Security Guidelines



The disciplinary process should be drawn up with the guidance of the organisation's human resources function and approved by the management team.