IT Checklist

Securing computers and electronic data:

- Disable Windows login account (server and/or local computer)
- Remove access to shared resources (network drives etc.)
- Reset passwords for any shared accounts and/or systems known by employee (shared logins, WiFi passphrases etc.)
- Archive / backup personal employee files

Remote access:

- Disable any remote access methods (websites, Remote Desktop, VPN etc.)
- Change Administrator passwords for all applications and accounts held by employee
- Obtain any special passwords unique to employee

E-mail related items:

- Remotely wipe mobile device if possible / appropriate
- Reset email account password
- Disable remote e-mail access
- Prepare Out of Office response
- Forward emails where appropriate
- Disable / delete email account when appropriate

Phone related items:

- Review and delete voicemail messages, backing up if necessary
- Delete voicemail account or change voicemail password
- Update voicemail directory
- Update phonebook advertisements and other directories

List updates:

- Update staff and department lists
- Remove employee name from letterhead / brochures
- Remove references to employee from Web sites
- Notify any relevant 3rd parties where employee may have privileges

Seek return of all firm property:

- Laptop
- Mobile
- Security pass
- Building and office keys
- Desk, file cabinet or file room keys
- Credit cards and calling cards
- Client lists

Investigation work

If available:

- Review email archive
- Review web activity
- Review file audit / remote access logs
- Review printing logs
- Review call logs (desk phone and/or mobile)

020 7099 9384 | foration.com | info@foration.com