|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ROLE: | Office IT Support Engineer | | CODE: |  |
| DIVISION/DEPARTMENT: | Finance | | LOCATION: | Reading, UK |
| ACCOUNTABLE TO: | Finance Director | | | |
| PURPOSE: | | | ORGANISATIONAL RELATIONSHIP: | |
| Manage and develop IT and Office systems and services used within the office environment including Data Center, Offices and cloud services (e.g. Azure, AWS).  Administer staff and contractor access to office IT systems and services for staff and external users as appropriate. | | | Primary reporting line to Finance Director for general staff management.  Secondary reporting line to Products Team Manager for technical direction.  Coordinating with direct colleagues and other members of the business for day to day systems issues. | |
| BUDGETS | | | | |
| DIRECT STAFF: | | 0 | REVENUE: | 0 |
| INDIRECT STAFF: | | 0 | CAPITAL: | 0 |

| ACCOUNTABILITY  (outputs, deliverables) | DECISIONS | MEASURES |
| --- | --- | --- |
| Office connectivity: Ensure system infrastructure provides high performance working environment.  Ensure systems are maintained on an on-going basis.  Implement changes where agreed with management. | Review infrastructure of current systems and decided what recommendations to put to Senior Management. | Remote desktop, Internet, telephone access and telephone conferencing is available during agreed office hours.  Colleagues are positive about the performance and suitability of the IT systems. |
| Administer systems access with following approval from HR. Includes email, SharePoint, CRM, website and Active Directory. | Assign people to roles as required and authorised by HR and line manager.  Determining when requests for access need to be approved by manager. | All users have minimum privileges for their roles.  Users do not have access that is not appropriate for their role. |
| Promptly set up hardware and system accounts and profiles for new starters or changes in accordance with instruction from HR. | Ensure equipment provided is adequate and not excessive. | All new staff have equipment and systems access ready for their first day. |
| Administer passwords and password resets requested by individuals where appropriate and ensure all staff understand the company policy for password management, providing assistance when necessary. | Ensure that the person requesting the password reset has authority to use the account.  Recommend use of strong passwords | System passwords are stored securely, regularly changed and unknown and un-guessable to others. |
| Take responsibility for continuous improvement of systems administration and IT Processes by leading on implementation of new systems. | Proactively assess current systems and make recommendations for improvements. With approval from Senior Management Team implement system changes. | New systems are assessed on an on-going basis against current and future operations. Appropriate systems are in place for all areas of the business. |
| Ensure all procedures for systems access are documented in SharePoint. | Review and update existing documentation. | Procedures are reviewed and tested accurately by a colleague.  All staff, especially new starters, can understand and follow documentation. |
| Monitor scheduled backups.  Where there are failures, or unexpected results, investigate and act or escalate as appropriate. | Understand outcomes that are cause for concern.  Determining whom should be notified when anomalies identified.  Investigate causes of failure and recommend actions to address. | Backups of Company’s systems and data are made at the documented frequencies and are available for restore whenever necessary.  Products Team Manager is informed of back-up failures.  All failures are successfully re-run to limit risk of data loss to 24 hours max. |
| Perform scheduled full system hard disk backups. | Consider day of week to run weekly backups through liaison with Data and Product teams. Ensure adequate stock of disks available. | Weekly backups are successful and disks rotated off site. |
| Test backups for integrity on a periodic basis | Consider when to perform back up tests. Investigate causes of failure and recommend actions to address. | Backup tests occur and the results are recorded in a form that can be audited.  Senior Management Team are informed of backup test failures. |
| Take responsibility for data storage and oversee offsite Data Centre activity and monitor Data Centre charges. | Recommend improvements to data storage, protection and spend. | There is always sufficient data storage available.  Obvious data efficiency errors are not missed. |
| Maintenance of office equipment including laptops, desktops, TVs, printers, telephones and mobiles. | Provide people with equipment as directed by Office Manager.  Identify when existing equipment is no longer fit for purpose. | Employees equipment functions as required to achieve their role.  Suitable stock of spares are maintained.  Lack of, or inadequate equipment does not impact the Company’s day to day operation. |
| Inventory of all office equipment is maintained and accurately recorded. Safety and security tests such as PAT tests take place as and when required. | Determine an efficient process to review the stock of IT equipment and ensure security and safety of that equipment is considered. | No item of stock is unknown by Financial Controller for depreciation/Insurance purposes. Security systems for protecting office equipment is established. |
| Work with HR Manager to ensure all staff can comfortably fulfil their legal and contractual IT obligations as part of the staff handbook procedures. | Determine an audit process to ensure all staff have ability to manage their IT legal requirements. Recommend training where required. | No member of staff fails to comply with staff handbook legal and contractual IT security obligations. |
| Regularly review MS Azure (and other similar) account, monitor usage and liaise with products team to keep costs to a minimum, whilst ensuring that the required level of service is also maintained. | Regularly review the Azure account usage, access anomalies or increased usage and investigate. | Expenditure on MS Azure account remains within budget.  Azure based services continue to operate within acceptable levels of performance and availability. |
| Promptly remove systems access for all leavers in line with company policy.  Completion and filing of Leavers Checklist when any employee leavers. | Ensure leavers checklist is updated with development of systems, and signed off with each leaver. | No ex-staff can access any part of the systems. |
| Maintain the companies Service Delivery plan so that it accurately reflects the physical infrastructure and services used to support the business. | Seek guidance from management if any questions about the document to processes. | The Service Delivery plan when audited, or used by colleagues to find out information, is always accurate and helpful. |
| Participate in the out of hours support rota equally with other technical staff providing 24/7 operation support for the Company’s core systems. | Work with the Product Manager to agree scheduled times considering holidays and other time out of the office for all colleagues.  Follow the out of hours support procedures taking appropriate action when alerts received, including escalation to management when necessary. | All out of hours incidents are dealt with according to company procedures. Impacted customers and colleagues are communicated with in a timely fashion.  Impact of Out of Hours systems outages is minimised. |

|  |  |
| --- | --- |
| ACTIVITIES  (Tasks to achieve accountabilities) | ACTIVITIES (cont) |
| Providing support for setting up a conference call.  Managing business landlines, mobiles and sorting out issues with a phone connection.  Provide a point of contact support with LAN and Internet related problems.  Setting up office hardware (printers, laptops, desktops, TV, etc.) and replacing parts as required.  Assigning users to groups as agreed by HR manager.  Making sure there are sufficient hardware resources to connect various devices (ex. Cables to connect a laptop or TVs).  Setting up accounts and systems’ access for new starters.  Ensuring that there is adequate hardware and systems capacity for planned new starters.  Revoking systems access for all leavers.  Travel to offsite Data Centre on a regular basis. | Installing and configuring computer hardware operating systems and applications.  Providing a basic technical support for 51Degrees employees (ex. Problem with accessing the remote desktops).  Sorting out 51Degrees email problems.  Managing users account (creating, disabling, deleting users’ account, resetting passwords).  Managing email, CRM and SharePoint accounts.  Taking backups of Company’s data as per defined procedures.  Ensuring that automatic backups have taken place at defined schedules.  Liaising with service providers (e.g. BT, data centre) when there are issues or changes required to provisioned services.  Ensure a structured and ordered store room with spares for all major equipment available.  Be available to participate in Out of Hours Support rota. |

|  |  |
| --- | --- |
| COMPETENCIES | EXPERIENCE |
| Good maths skills. GCSE C or above.  Good written and spoken English skills.  Willingness to learn and be part of a successful team.  Pro-activity – must be able to take initiative, pre-empting potential problems and trying to identify solutions to problems.  Approachable – colleagues should feel comfortable about asking you for help. | Degree level or equivalent understanding of general computing concepts.  Experience of windows operating systems and home office networking. |