|  |  |
| --- | --- |
| **Job Title** | Cyber Security Operations Manager |
| **Reports to** | Head of IT Services |

**Job Purpose**

The IT Infrastructure Department provides, manages and supports all aspects of IT life at the College. The role of the Cyber Security Operations Manager is to manage the security and resilience of all Eton’s data and equipment, ensuring the College’s operations operate to their fullest abilities, and that Eton’s data and operations remain secure and protected.

**Key Tasks and Responsibilities**

* Overarching management of the security of Eton’s IT environment, whether physical or virtual, on-premise or hosted off-site;
* Overarching management of the security of Eton’s data, whether hosted on-premise or off-site;
* Work alongside the IT Infrastructure Manager in all infrastructure projects, but retain ownership of the security aspects of any such project;
* Work alongside the Networking team in all networking projects, but retain ownership of the security aspects of any such project;
* Strategic planning of the School’s IT security, working alongside the IT Infrastructure Manager as appropriate;
* In co-operation with other senior member of the IT Department, develop and implement policies and procedures for IT security matters;
* Monitor and provide regular reports on the security of Eton’s IT environment;
* Manage and maintain all security appliances and software systems deployed on the College network;
* Create and provide regular reports on the security of the College’s systems and data, any threats to which the College is vulnerable or has been subjected, and any actions taken;
* Specify, deploy, manage and maintain any security system or process aimed at protecting Eton’s systems, data, interests or reputation;
* Make recommendations to the Heads of IT of any changes or additions to Eton’s IT environment that would improve the security of data or systems;
* Maintain a working knowledge of the role of the IT Infrastructure Manager, in order to assist or provide cover, if required;
* Ensure all aspects of the College’s IT security are accurately documented, and that this documentation is regularly updated and available to other members of the IT department;
* Provide regular training to the College’s user base on cyber security, advising staff and pupils on best practices and explaining systems and processes in place for their protection;
* Keep up to date with current and emerging threats, trends and industry best practices;
* Work as directed by the Head of IT Services;
* Be a highly motivated team player with the skills and ability to manage changing priorities;
* Be willing to attend internal and external training as necessary to keep up to date with the latest technology and internal system processes;
* Work within industry standard legislation, policies and procedures;
* Undertake other duties not specifically stated which from time to time are necessary without altering the nature or level of responsibility.

**General & College Responsibilities**

* Participate in training and team development activities, to update knowledge and skills:
* Be aware of and comply with the health and safety legislation and other College requirements that are relevant to their post.
  + All employees have a general duty in law to take reasonable care for the health and safety of themselves and of other persons who may be affected by their acts or omissions.
  + Understand and be committed to the College’s Health and Safety Policy statement and the College’s safety priorities and be aware of their contribution to such priorities
* Demonstrate commitment and enthusiasm to promote the principle of equality and diversity in employment and service delivery:
  + Be familiar with and promote the Equality and Diversity Policy.
* Be familiar with Safeguarding requirements as outlined in the Safeguarding Policy and comply with its requirements to safeguard and protect the welfare of children, young people and vulnerable adults.
* Undertake such additional duties or projects as the Head of IT Systems may determine from time to time, after consultation with the post holder.
* Where required, undertake regulated activity, such as unsupervised contact with children, ensuring that safeguarding procedures are followed and providing safe and effective care at all times.
* Good understanding and effective implementation of Child Protection procedures
* Commitment and promotion of equality, diversity & inclusion
* Commitment to safeguarding and promoting the welfare of children, including by not limited to, completing safeguarding training as required, and ensuring any safeguarding updates issued by the College are read and understood.
* Understand and comply with procedures and legislation relating to confidentiality.

**Skills and Competencies Required**

To be successful in this role, the incumbent should have:

* Excellent knowledge of Microsoft Windows Server Operating Systems, version 2008 and later;
* Competence with computer, server and peripheral hardware;
* Excellent knowledge of networking topologies, standards, terminologies and operation;
* A thorough understanding of the cyber security threat landscape;
* A good standard of written and oral communication;
* Ability and willingness to provide user training on security topics, whether in an individual, group or forum setting;
* Ability to work effectively within a team environment, both taking direction from and supporting other colleagues.
* Excellent technical skills and a friendly and helpful manner;
* A demonstrable aptitude and enthusiasm for information and communications technology;
* Confidence and willingness to build on knowledge acquired to date;
* Good communication skills and ability to work well in a team environment;
* Ability to organise and prioritise workloads.

**Working Pattern**

* Your usual working hours will be 9am to 5pm, Monday - Friday with 1 hour for lunch. These hours are not fixed and some flexibility is required as a response to peaks in workload.
* You will be working 52 weeks per year.
* You will be entitled to 24 days of holiday. (You must use all your entitlement (including any lieu days) during periods of school holidays. If a bank holiday falls during a school term period, you will be required to work this day and you will receive an additional day’s holiday in lieu.)
* Any remaining weeks, save as outlined in your annual leave provisions below, are deemed to be non-working weeks.

**Disclosure Checks**

Eton College is committed to safeguarding and promoting the welfare of its students and staff and expects all staff and volunteers to share this commitment. This role is classed as ‘regulated activity’, whereby the post holder may be required to have contact or be involved in unsupervised activities with children. It is a criminal offence for any person who is barred from working with children to attempt to apply for a position at the College. The suitability of all prospective employees will be assessed during the recruitment process in line with this commitment.  All offers of employment are subject to a number of recruitment checks, including by not limited to; verification of identity and right to work in the UK, an Enhanced DBS check, pre-employment health check questionnaire, satisfactory references, verification of professional qualifications which the College deems a requirement for the post, or which were otherwise cited in support of your application and probationary period.