

ROYAL HOLLOWAY, UNIVERSITY OF LONDON

NorthgateArinso Hosted My View Security Statement

NorthgateArinso take the security of customer's data and our systems very seriously. You may notice the padlock symbol when using the MyView application; this is because NorthgateArinso uses the same method for protecting your personal details as on-line Banks. The use of the HTTPS network protocol encrypts network traffic making it virtually impossible to intercepted and read by a third-party. Also, for personal information, no data is left behind on your PC after you view a web page. A user must login using a valid user name, password and if required, the answer to a number of security questions. The answers to the security questions are encrypted in the system and therefore support staff cannot see this data. Authentication (to verify who you are) comes from either inside the ResourceLink HR system or externally using an existing Directory Service such as Active Directory or LDAP. This latter method allows you to use your network user ID and password.

In order to ensure that MyView self-service continues to meet the highest security requirements, NorthgateArinso has commissioned independent third-party penetration tests by Symantec Corporation of the application software. These tests are carried out at least annually or when there is a major release of software. The objective of the tests is to identify and prioritise potential areas of security vulnerability. The tests are based upon application settings and recommendations by OWASP, the Open Web Application Security Project (<http://www.owasp.org/index.jsp>) for implementing and developing web applications. A Management Summary of this report is available to your Management under Non-Disclosure Agreement.

Our Hosting infrastructure is of Enterprise class using industry leading, highly resilient hardware and software. Our choice of technical platform is much less vulnerable to attack than commodity environments, but nonetheless we have a number of significant countermeasures in place. NorthgateArinso have two secure data centres, one for production systems and another for Disaster Recovery. Both are purpose built facilities having extensive 24x7 physical security (guards/patrols, access controls, CCTV, environmental controls etc.) and logical security (firewalls, intrusion detection/prevention systems etc.). Data is replicated between data centres on an ongoing basis and encrypted backups are undertaken daily from the DR data centre.

NorthgateArinso has achieved two significant standards for security which are independently audited at least annually: ISO27001, an internationally recognised standard for Information Security and SAS70 (Statement on Auditing Standards No. 70), a widely recognised auditing measure for service organisations developed by the American Institute of Certified Public Accountants (AICPA). NorthgateArinso has the more demanding Type II certification. The hosting infrastructure is subjected to monthly vulnerability scans and bi-annual penetration tests by an independent third-party consultancy. Management summaries of these reports are available to your Management under Non-Disclosure Agreement. The Northgate Group's Information Security Manager is responsible for creating and maintaining our Information Security Management System (ISMS). The Information Security Steering Group (ISSG) comprises representatives from each business area and is chaired by the Chief Information Officer. The ISSG is responsible for reviewing Northgate's security policies. The ISMS is compliant with the international standards and code of practise ISO 27002.

NorthgateArinso recognises its legal and moral duty in processing personal data, by ensuring that data is handled properly and confidentially at all times and with due respect for the privacy of the individuals whose data is being processed. Our customers can be assured that the data will be treated in line with the eight principles of the Data Protection Act. Northgate has full security audit and can assure our customers that data will not be used inappropriately and will be properly and professionally managed.