

## **BEACON Security Statement**

The BEACON system utilizes 128-bit encryption via SSL (Security Socket Layer) technology to ensure that employee data is securely transmitted between the BEACON server and an employee's web browser.

The SSL protocol has been approved by the Internet Engineering Task Force (IETF) as a standard, and is widely used by financial organizations for on-line banking and investing, as well as by companies offering on-line purchases by credit card.

No one else can access an employee's personal data via the BEACON Portal other than the employee. To log on to the system an employee must enter her NCID and the password she created. The State's human resources professionals, with the proper security clearance, can only access employee personal data using the state network through the BEACON back-end system.

The BEACON databases are secured within the state network under compliance with statewide security standards put in place by the North Carolina Office of Information Technology Services (ITS) Enterprise Security and Risk Management Office. The BEACON system complies with all statewide security policies and guidelines to ensure that your personal data is protected.

### **To further protect sensitive information, employees:**

- Should create a password that is not easily guessed by others and is a mixture of upper and lower case letters, combined with numbers and/or special characters (NCID requires a minimum of 8 characters and at least 1 special character)
- Should close their browser after logging off
- Should ensure the browser they are using is Internet Explorer 6.0 with Service Pack 1 or Internet Explorer 7.0
- **Should not** share their password with others or write it down and leave it in the open
- Should notify the Risk Mitigation Services/Security Liaison within 30 minutes if you believe someone is attempting to gain unauthorized access to the system.