

## OSC HR/Payroll Security Statement

If you suspect or witness a security weakness or breach; or you suspect or know that confidential information has been disclosed or misused (or is about to be), you must immediately notify your agency's Security Liaison or contact BEST Shared Services at **919-707-0707** or toll free at **866-622-3784** to report the incident.

## Privacy and Confidentiality

Every person has a fundamental right to privacy and confidentiality. This policy defines, identifies and establishes the key components regarding management of confidential information by OSC HR/Payroll personnel. This policy pertains to all oral, paper based and electronic confidential information. OSC abides by the States information security policies detailed in the Statewide Information Security Manual (<https://www.scio.nc.gov/mission/itPoliciesStandards.aspx>).

We are committed to maintaining privacy and confidentiality, and recognize the need for appropriate protection and management of any personal information (social security number, personal address and telephone number, email, bank account numbers etc.) you provide to us. While much of the information housed in the OSC HR/Payroll is required to perform HR and Payroll functions due to federal and state regulation, we do collect discretionary information with the consent of the employee. We will protect personally identifiable information and discretionary information; we will keep it confidential and will not sell, license or disclose personal information to any third party unless we are compelled to do so under the law or to comply with a court order.

OSC HR/Payroll collects personally identifiable information, such as your e-mail address, name, home or work address or telephone number. OSC HR/Payroll also collects anonymous demographic information, which is not unique to you, such as your ZIP code, age, gender, and veteran status. OSC HR/Payroll collects and uses your personal information to operate the HR/Payroll system and deliver the services you have requested.

Employees are responsible for updating demographic information, which includes current address and telephone number, emergency information, tax withholding information, bank accounts, benefits data, e-mail address via NCID, and emergency contact information. Employees may also contact their Human Resources department for updates to their personnel records.

**Note:** It is important that employees monitor their employee records and notify their Human Resource department of discrepancies to maintain the quality and integrity of their personnel data.

HR/Payroll data may be stored indefinitely. State and federal regulations set the minimum durations for storing certain types of data based on tax rules, retirement calculations and various other processes that dictate data retention.

Please note that employee's personnel records are confidential in accordance with the Privacy of State Employee Personnel Records Act, NCGS §126-23, except that the following information is public about every employee:

- a. Name;
- b. Age;
- c. Date of original State employment or appointment to State service;
- d. The terms of any contract by which the employee is employed whether written or oral, past and current, to the extent that the agency has the written contract or a record of the oral contract in its possession;
- e. Current position;
- f. Title;
- g. Current salary;
- h. Date and amount of each increase or decrease in salary with that department, agency, institution, commission, or bureau;
- i. Date and type of each promotion, demotion, transfer, suspension, separation, or other change in position classification within that department, agency, institution, commission, or bureau;
- j. Date and general description of the reasons for each promotion with that department, agency, institution, commission, or bureau;
- k. Date and type of each dismissal, suspension, or demotion for disciplinary reasons taken by the department, agency, institution, commission, or bureau. If the disciplinary action was a dismissal, a copy of the written notice of the final decision of the head of the department setting forth the specific acts or omissions that are the basis of the dismissal; and
- l. The office or department to which the employee is currently assigned.

Salary information includes pay, benefits, incentives, bonuses, and deferred and all other forms of compensation paid by the employing entity.

All OSC HR/Payroll personnel are required to comply with the Security, Privacy and Confidentiality Policies. OSC HR/Payroll personnel shall immediately report to their supervisor any violations of this policy. OSC HR/Payroll personnel that fail to comply may be denied further access to confidential information and may be subject to disciplinary action up to and including termination.

## **Security Measures**

The BEACON system utilizes 128-bit encryption via SSL (Security Socket Layer) technology to ensure employee data is securely transmitted between the BEACON server and a 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; and companies offering on-line purchases by credit card.

Employees are given access to their personal data via the BEACON Portal using his/her NCID and a password known only by the employee. The State's human resource professionals, with the proper security clearance, can 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 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 contains a mixture of upper and lower case letters, combined with numbers and/or special characters (NCID requirements will guarantee a strong password).
- Close the browser after logging off.
- Use Internet Explorer browser.
- Do **not** share their password with others or write it down and leave it visible to others.