PHYSICAL AND CYBER SECURITY POLICY

1. OVERVIEW

The protection of both physical and cyber assets is a core value for the Iconic Power System (IPS) management team. An unauthorized physical or cyber access to IPS's facilities, servers, or IPS information, as defined in the Information Security Management Policy, could significantly impact IPS's reputation with its clients, employees, and lead to potential regulatory penalties or legal action.

2. PURPOSE

The purpose of this policy is to establish the requirements for physical security at IPS facilities and customer sites, and to ensure cyber protection is in place to mitigate the risk of a cyber breach, resulting in a loss of IPS assets or information/data.

3. SCOPE

This policy is applicable to all employees, contractors, and visitors to IPS facilities or IPS managed customer sites.

4. POLICY

4.1 Physical Security at IPS Office

The corporate facilities will have the appropriate level of physical security requirements based on the potential risk of unauthorized entry or access to the facilities, loss or theft of information, and overall security threats.

All visitors to the IPS office are required to sign in and out of the visitor log book. They must also show valid government issued picture identification to allow IPS to verify their identity and must wear an IPS visitor badge.

IPS will have a **Physical Security Plan IPS-SEC-PLN-CON-004** based on a physical security assessment. This plan will be formally reviewed every two years or when circumstances arise which require a revised assessment (e.g., after an event, significant increase in resources, new threat, etc.).

To protect physical information or data within the corporate office, refer to the Information Security Management Policy.

4.2 Physical Security – Customer Site

A **Field Security Plan IPS-SEC-PLN-CON- 004** will be developed for all customer sites. The plan is required to assess and proactively mitigate possible threats prior to the commencement of the work.

The security plan will include the following:

- A site risk assessment conducted with the customer to assess the threat level in the region or based on the type of work being performed.

- When third party contractors are performing work on behalf of IPS, i.e. subcontracted, they will also be part of the risk assessment.
- All additional physical controls required to mitigate the threats identified as part of the risk assessment (e.g. additional fencing, security guards, security cameras, locked storage areas such as c-cans, specific work procedures, equipment storage or additional locking, access controls, etc.).

4.3 Physical/Cyber Security – Critical Infrastructure Protection Customer Site

In addition to 4.2, IPS employees and contractors will need the meet specific requirements defined by the customer at Critical Infrastructure Protection (CIP) Facility. The minimum requirements are defined as follows but can be changed by the customer at any time, thus always confirm the requirements with the customer:

- A valid criminal background check and identity verified to be renewed every 7 years
- Annual CIP training as defined by the customer requirements
- Approval by the customer to have electronic access to their LAN when working on RTUs, Relays or HMIs at these sites
- And/or approval by the customer to have Unescorted Authorized Access to the Physical Security Perimeters within the CIP Facility.
- Or, if an employee or contractor does not meet the requirements set in this section for unescorted authorized access, they will be considered a “visitor” by the customer and therefore the contractor or an IPS employee/supervisor will need to ensure they have at least one individual at the site who can keep the “visitor” within line of sight at all times during the work.
- Documentation of access to the CIP facilities is owned and managed by the AltaLlink. However, IPS has responsibilies to comply with the requirements of the contract with AltaLink. These requirements are detailed in the **Provision Access Process IPS-SEC-PRO-CON-001, Personal Risk Assessment for BCSI/CIP Access Process IPS-SEC-PRO-CON-002, and BCSI/CIP Access Process IPS-SEC-PRO-CON-003.**
- Note that if either IPS and/or the contractor terminate an employee working at AltaLink CIP customer sites, IPS and/or the contractor must notify them within 6 hours of termination (this timeline is defined in the contract terms with customer and must be met). For more information refer to the **Revocation and/or Change of Access Process IPS-SEC-PRO-CON-005**.
- For AltaLink the contact numbers are as follows:
  Service desk - 403 267 4444 or 1-866-258-2565 (24 hours)

  Security desk – 403 267 4495 (24 hours)

  NOC – 403 387 8299 (Between the hours of 7:30AM and 4:00PM)

  ACC – 403 267 1520 (between the hours of 4:00PM and 7:30AM)
- This policy will be updated based on the addition of contract with other utilities or generating facility operators who require compliance to the CIP Alberta Reliability Standards.

4.4 Cyber Security

This section of the policy refers to all policies which detail the cyber protection minimum requirements for all IPS employee and contractors which must be meet to protect IPS cyber assets.

As per the physical security section 4.1 the Information Technology (IT) servers have additional physical protection, see Server Protection Policy and Wi-Fi is protected as per the **Wireless Communication and Connection Policy and the Password Protection Policy IPS-SEC-POL-CON-008**.

All information must be classified and protected as per the Information **Security Management Policy IPS-COR-POL-PBC-003.**

All servers and emails will be protected as per the **Anti-Virus and Malware Policy IPS-SEC-POL-CON-003.**

All BCSI information, in transit by third party contractors, will be encrypted as per the **Encryption Policy IPS-SEC-POL-CON-009.**

All access BCSI information stored on IPS servers must be controlled as per the **Remote Access Policy IPS-SEC-POL-CON-006.**

All access must be managed as per the Remote Access Policy.

All software and hardware installation must meet the requirements of S**oftware and Hardware Installation Policy IPS-SEC-POL-CON-007** .

IPS network servers must meet the requirements of the **Server Protection Policy IPS-SEC-POL-CON-005**.

5. POLICY COMPLIANCE

5.1 Compliance Measurement

The IPS Health, Safety, Security and Environment (HSSE) Manager will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, internal and external audits, and feedback to the policy owner.

5.2 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, as per the **Disciplinary Policy IPS-HSE-POL-PBC-003**.

6. REPORTING OF NON-COMPLIANCE, BREACH OR POTENTIAL BREACH

It is important for employees and contractors to report actual events as well as near misses. IPS management values the learnings gained from near misses or potential cyber/physical breaches or events.

Employee and contractor must report any non-compliance or potential non-compliance to this policy and the associated security policies to the HSSE Manager, or President.

For any potential or actual physical and/or cyber breach refer to the ***I*nformation/Data Breach Policy IPS-SEC-POL-CON-002, the Health Safety and Environment (HSE) Investigation Policy, the HSE incident Reporting Policy and/or Physical and Cyber Security Incident Classification Standard IPS-SEC-STA-PBC-001 for further details on investigation requirements.**

7. REFERENCE POLICY, PROCESSES, PLAN, STANDARD AND FORMS

- Acceptable Use Policy IPS-HRS-POL-PBC-001
- Anti-Virus and Malware Policy IPS-SEC-POL-CON-003
- Disciplinary Policy IPS-HSE-POL-PBC-003
- Encryption Policy IPS-SEC-POL-CON-009
- Information Security Management Policy IPS-COR-POL-PBC-003
- Information/Data Breach Policy IPS-SEC-POL-CON-002
- Password Protection Policy IPS-SEC-POL-CON-004
- Remote Access Policy IPS-SEC-POL-CON-006
- Software and Hardware Installation Policy IPS-SEC-POL-CON-007
- Server Protection Policy IPS-SEC-POL-CON-005
- Wireless Communication and Connection Policy IPS-SEC-POL-CON-008

- Provision Access Process IPS-SEC-PRO-CON-001
- Personal Risk Assessment for BCSI/CIP Access Process IPS-SEC-PRO-CON-002
- BCSI/CIP Access Process IPS-SEC-PRO-CON-003
- Revocation and/or Change of Access Process IPS-SEC-PRO-CON-005
- Physical and Cyber Security Incident Classification Standard IPS-SEC-STA-PBC-001

- Physical Security Plan IPS-SEC-PLN-CON-003
- Field Security Plan IPS-SEC-PLN-CON-004

- Risk Assessment Policy IPS-COR-POL-PBC-002
- Risk Assessment Process IPS-COR-PRO-PBC-001
- Risk Assessment Matrix IPS-COR-TMP-PBC-001