Carolus XIII

Royo y Imperad

A.S. 325

* *

No.1 of 2025

An Act relating to the Protection of Official Secrets from Inappropriate and Harmful Disclosure.

Given Sanction on the 31st of January, 2025

SARHOLM

Maya seo donir plisir eun Seito Majis Imperial y Stefanica, pur Seito Majis y pul y pur tel consei y sazion eui tel Parlarmente eui tel Rozirre, comaria tel segeoare:

1. Short Title This Act shall be known as the *Official Secrets Act of 325 AS* in short.

2. Preamble In recognition of the need to safeguard the security, sovereignty, and integrity of the nation, this Act establishes the framework for the protection of classified information critical to the public good. It delineates the responsibilities of individuals and institutions in preserving state secrets, preventing unauthorized disclosures, and ensuring the proper handling of sensitive materials. Through these measures, the Act seeks to uphold national interests, promote trust in governance, and fortify the nation's defense against internal and external threats.

2. Authority of Classification All documents and information published by His Imperial Majesty's Stationery shall receive security classifications jointly at the discretion of the Prime Minister of New Sarovia and the Crown Intelligence and Security Agency, based on the potential harm to national security, impact to the international and domestic relations of New Sarovia, risk to any individual privacy and the effect on military or civil operations.

Classification decisions must be recorded with basic justification, as well as reviewed when necessary; and made public to relevant departments.

3. Tiers and Classifications There shall be four types of security clearances - *Unrestricted*, *Protected*, *Secret* and *Top Secret*. They shall be the official national security classifications and are subject to a memorandum of understanding between all states and the Sarovian Government.

A security classification (*Protected*, *Secret* and *Top Secret*) is only applied to information (or assets that hold information, such as servers, channels, DM conversations) if it requires protection because the impact of compromise of the information or asset would be high, extreme or catastrophic.

Unrestricted shall apply to all documents, channels and information that are freely published by His Imperial Majesty's Stationery, and do not need to be explicitly classified as *Unrestricted,* but may be. *Protected* shall mean unauthorised disclosure will cause damage to the national interest, organisations or individuals. *Secret* shall mean unauthorised disclosure will cause *serious damage* to the national interest, organisations or individuals.

Top Secret shall mean unauthorised disclosure will cause *exceptionally grave damage* to the national interest, organisations or individuals. All documents and written conversations between Ministers, including DMs, Cabinet discussions, voice calls are automatically considered *Top Secret.*

4. Security Clearances A security clearance shall be a statement of assurance that a person is both eligible and, so far as can be determined at the time that the clearance is issued, suitable to hold a position of trust that gives them access to security classified Sarovian Government information, resources and activities.

It is a point in time judgement that must be accompanied by ongoing security management of those holding clearances to ensure that they remain suitable. Individuals who require ongoing access to Sarovian Government security classified information, resources and activities must hold a security clearance, commensurate with their security classification. The security clearance level required is not based on the person's rank, seniority or status, but on the necessary access required to perform their identified position.

An active security clearance is sponsored and maintained by the Crown Intelligence and Security Agency. All Commissioned Officers of the Imperial Sarovian Armed Forces and all Lord-Lieutenants, Members of Provincial Parliament and Members of the Imperial Parliament are automatically awarded *Protected* clearance upon the recipient of their commissioning scroll or their Oath of Allegiance. Members of Parliamentary Committees may receive *Secret* clearance for their specific committee.

5. Authorised Vetting Agencies

The Imperial Sarovian Constabulary will, on order from the Crown Intelligence and Security Agency, conduct security vetting for Sarovian Government entities, unless the entity has been authorised to conduct security vetting for its own personnel. The Imperial Sarovian Constabulary must conduct security vetting in a manner consistent with this Act. The term 'vetting analyst' denotes a person within CISA who reviews vetting assessments established by the Imperial Sarovian Constabulary.

The Rosecuizo, or a security vetting delegate, is formally authorised to make decisions on the outcome of a vetting process (i.e. to grant, deny, grant-conditional, revoke or cancel a security clearance).

6. Eligibility for a Security Clearance

To be eligible for a Sarovian Government security clearance, an individual who does not automatically obtain their clearance through their occupation must be a Sarovian citizen for a minimum three Stefanic years, and be sponsored for vetting by a cleared individual. The Crown Intelligence and Security Agency may deem a background as 'security uncheckable', permanently refusing them security clearance.

The Crown Intelligence and Security Agency will assess Sarovians subject to security vetting based on the following characteristics:

a) Honesty and integrity.
b) Maturity and judgement.
c) Stability and reliability.
d) Tolerance and acceptance.
e) Loyalty and commitment to Sarovia, its values and its democratic system of government; and
f) Vulnerability to improper influence or coercion.

7. Disclosure Requirements

Clearance subjects must provide explicit informed consent to share the information required. At minimum and under an oath of truth, Sarovians subject to security vetting must, if required, provide the Imperial Sarovian Constabulary who will provide concerns to the Crown Intelligence and Security Agency, with:

a) Discord activity for the past six (6) Stefanic years; including
    i) Other Discord servers;

ii) Ties to foreign powers;
iii) Significant friendships or relationships made in other servers or organisations;
iv) Relevant affiliations in any other national membership for the past 12 Stefanic years,
v) Roles in any online community;
vi) Friendships with foreign officials; and
vii) Rivalries or conflicts with neutral, friendly or enemy states.

8. Verification Requirements

The Imperial Sarovian Constabulary will verify these disclosures through a manual review of accessible Discord history and provide the Crown Intelligence and Security Agency their verdict. The Imperial Sarovian Constabulary may also interview any individual mentioned within these disclosures.

9. Violations

Minor violations shall be defined as the unintentional omissions of non-critical information within disclosures; delays in reporting changes (less than 14 days late); accidental sharing of *Protected* information with unauthorised persons; miscommunication about server roles or relationships that does not impact security and sharing of *Protected* information with unauthorised persons.

Serious violations shall be defined as any intentional false declaration to vetting agencies; any omission of foreign nation affiliations, leadership roles in other communities, known conflicts with cleared individuals, previous security incidents; sharing of *Secret* or *Top Secret* information with unauthorised persons; pattern of repeated minor violations (3 or more in 6 months); failure to report known security violations by others; active concealment of relevant information; any violation of the provisions defined in this Act.

Minor violations shall be decided by the Crown Intelligence and Security Agency, which may instruct or delegate instruction to the wrongdoer that they have been sanctioned. Sanctions shall be:

a) First offense shall constitute a written warning;
b) Second offense shall constitute the suspension of clearance for a period of 2 Stefanic years; and
c) Third offense shall be treated as serious violation.

Minor violations shall be decided by the Crown Intelligence and Security Agency and approved by the Court, which may instruct or delegate instruction to the wrongdoer that they have been sanctioned if found guilty. Sanctions could be:

a) Immediate and clearance revocation;
b) 12 Stefanic year minimum ban from reapplication;
c) Public notice of clearance revocation;
d) Loss of current government positions where legally applicable;
e) Ban from government service for 24 Stefanic years;
f) Fine of 50,000 Saros; and
g) A review for violations of criminal charges under the Mathievas Code of Law Sections 6 and 8, or others if applicable.

10. Accidental Disclosure

Unintentional omissions that are self-reported before discovery, or corrected within 7 days, or not related to critical security matters may be treated as administrative matters rather than violations, at the vetting agency's discretion.

If any information that is tiered above *Unrestricted* is accidentally disclosed, the person discovering the disclosure must:

a) Stop sharing immediately;
b) Report to CISA within 24 hours; and
c) Document all who may have seen it.

11. Information Sharing

Information can only be shared between people with security clearances at the same level or higher, and only if both parties have a legitimate need to know. The sharing of information to individuals that cannot be justified as a legitimate need to know may be prosecuted as a major or minor sanction.

12. Emergency Sharing

In the event of an emergency, which shall be defined as any immediate threat to national security or interests; ongoing security incidents, critical diplomatic situations, martial necessity or a threat to any personal safety, members in the Cabinet, General Staff or Navy Admiralty with *Top Secret* access may share classified information with individuals unqualified to possess this information. The sharer of the information must, within sixty minutes of sharing this information, report this to the Prime Minister, with a detailed justification for the emergency, any and all steps taken to limit exposure and a plan to control further information leaks. These reports will be reviewed by the Crown Intelligence and Security Agency, which will determine if the emergency was justified and the individual took all reasonable steps to ensure the limit of information exposure.

13. Information Control Measures

Any shared information that requires specific controls and handling procedures must be clearly marked as *Protected, Secret* or *Top Secret*.

For temporary access, the information must be prefixed with "TEMP ACCESS" and include both handling instructions and an expiration date. Upon receiving classified information, recipients shall acknowledge receipt and explicitly confirm their understanding of any restrictions. Recipients are prohibited from resharing the information without obtaining new authorisation, must remove or restrict access when the sharing period expires, and are required to report any unauthorised access immediately.

14. Appeals Process

Clearance denials may be appealed within 14 days by:

a) Submitting written explanation;
b) Providing new information; and
c) Requesting sponsor testimony.

Appeals will be reviewed by the Crown Intelligence and Security Agency alone.

15. Maintaining Clearance

All clearance holders, once a month, will be approached by a member of a vetting agency in order to collect any information on new server memberships, relationships with foreign officials, personal conflicts, government roles and any other additional information.