

General Policies Procedures and Rules for Tritium Cyber Defence

AUNA:Anthony Grace

AUID:MD01S01

OVER-STATEMENT:

- Membership within TRITIUM CYBER DEFENCE requires agreement and sign off on the following rule sections:

GENERAL MORAL CODE:

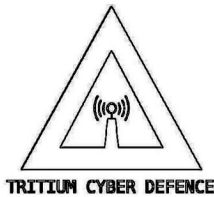
- Tritium members will conduct **ethical hacking only** and will **not** attempt, commit, or conspire criminal offences. See:
 - PRIVACY ACT 1988
 - CRIMINAL CODE ACT 1995
 - Parts 10.7 and 10.8
- Uprstanding character and attitude.
- Academic rigour and strong work ethic.
- Abstainment from the use of illegal drugs or abuse of drugs.
 - Especially during development or work projects.
- Working towards a stronger team environment and growth of themselves and Tritium.
- Members shall not destroy any software, hardware, or property of Tritium or its members except under written and signed approval from **ID:MD01S01**

COMMUNICATION:

- Members will conduct communication with each other and clients in a friendly, kind, and helpful way.
- Criticism must be done in a constructive manner.

REQUIREMENTS FOR MEMBERS:

- A personal GitHub repository and account.
- Persistence with online training.
- Persistence with development projects.
- Dedication to cybersecurity matters and duties.
 - “Playing an active role”.



General Policies Procedures and Rules for Tritium Cyber Defence

AUNA:Anthony Grace
AUID:MD01S01

CARDINAL RULE:

- Addherance to the Criminal Code Act 1995. See parts 10.7 and 10.8:
 - DIVISIONS 476 TO 480

****Possession or control of hardware, software, or other tools with the intention to commit an offence against Division 477 as above.****

“Our creation and research of the hardware, software, and tools are strictly to be used under authorisation from a section leader and only to be detonated/ deployed on systems authorised by their owner. All storage of the developed tools must be on a private, encrypted repository or other secure method such as:
‘keybase encrypted storage’ or ‘GitHub private repos’”
-TRITIUM CYBER DEFENCE STATEMENT-

REPRIMAND:

- Faliure to adhear to the above values and rules can result in disiplinary action and/ or termination from Tritium Cyber Defence.
- Faliure to adhear to the cardinal rule above will result in serious **legal penalty including imprisonment.**

**DOCUMENT END
NO PTO**