



Do not  
punish employees  
who made a  
genuine report of  
**SIGNS OF CONCERNS**,  
even when it  
turns out to be a  
wrong interpretation

Measure Observation 26



**REWARD  
EMPLOYEES**  
who report signs  
of concern

Measure Observation 1



Have different  
**REPORTING**  
mechanisms

Measure Observation 2



Have  
**SECURED ENDPOINTS**  
or access points  
for the end user,  
such as desktops,  
laptops, and mobile devices  
(*'endpoint security tools'*)

Measure Observation 3



Create a  
**REPORTING CULTURE**  
where employees  
know they are  
**HELPING  
THEIR COLLEAGUES**  
when they  
mention their concern

Measure Observation 4



Create a  
**SUPPORTIVE CULTURE**

Measure Observation 5



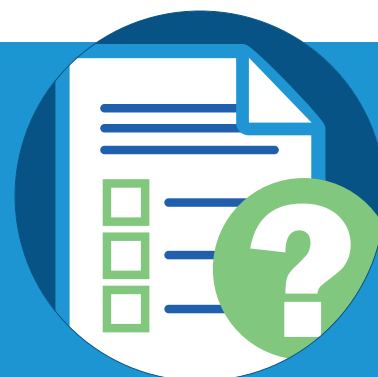
Conduct  
**DESKTOP  
SIMULATIONS**

Measure Observation 6



Stress that  
**HOLIDAYS AND TIME OFF**  
from work are to be  
used regularly

Measure Observation 7



Have an  
**ANONYMOUS**  
internal reporting system

Measure Observation 8



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



Have a  
**HOTLINE**  
to mention  
signs of concern

Measure Observation 9



Organize  
for an  
**EXTERNAL AUDIT**  
to be carried out

Measure Observation 10



Physical  
and technical  
**SECURITY  
MEASURES**

Measure Observation 11



Use  
**ARTIFICIAL  
INTELLIGENCE/  
MACHINE LEARNING**  
to detect signs of concern  
*(UEBA, Anomaly Detection,  
Sentiment Analysis, Keyword Matching)*

Measure Observation 12



Use  
and audit systems  
to assess the use of  
**BADGES/ACCESS RIGHTS**  
*(electronic access control)*

Measure Observation 13



Use a  
**FORMAL ASSESSMENT**  
process  
supported by  
recurring sessions (yearly)

Measure Observation 14



Management  
**APPROVAL**  
necessary for  
potential disruptive actions

Measure Observation 16



**REPEAT SCREENING**  
when employees  
are set in a more  
vulnerable position

Measure Observation 17



**IDENTIFY  
THE ASSETS**  
of the  
organization

Measure Observation 18



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



Encourage isolated  
or less socially  
active employees  
to take part in  
**INFORMAL GATHERINGS**

Measure Observation 15



Install a  
**CONTACT POINT**  
to report signs of concern

Measure Observation 19



Carry out an  
**INTERNAL AUDIT**

Measure Observation 20



Invest in a  
culture of open  
**FEEDBACK**  
and trust

Measure Observation 21



**ROTATION**  
of jobs

Measure Observation 22



Let  
**SECURITY**  
report directly  
to the CEO

Measure Observation 23



Let  
employees work  
in  
**TEAMS**

Measure Observation 24



Put the  
responsibility for  
**MONITORING**  
behavior  
with all employees,  
not only with  
the security team

Measure Observation 25



**INVESTIGATE**  
the use of  
internet  
and  
social media activity

Measure Observation 27



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



Develop a  
formal  
**THREAT ANALYSIS**  
for insiders

Measure Observation 28



**INVESTIGATE**  
the  
work climate  
periodically  
and  
variably

Measure Observation 29



Organize a  
periodic and variable  
**PSYCHOLOGICAL  
ASSESSMENT**  
*('fitness for duty')*

Measure Observation 30



Put  
**ALARMS**  
on the access system

Measure Observation 31



**RED-TEAMING**

Measure Observation 32



**RISK ANALYSES**  
based on  
access and impact

Measure Observation 33



Separation of  
**ROLES AND TASKS**  
*('separation of duties')*

Measure Observation 34



**STRUCTURAL  
COORDINATION**  
and  
**COMMUNICATION**  
throughout the  
organization

Measure Observation 35



**TEST  
VULNERABILITIES**  
of employees  
for manipulation  
of a hostile third party  
*('social engineering')*

Measure Observation 36



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation





Set up  
**TOOLS**  
for  
prevention of data loss  
(DPL)

Measure Observation 37



**ORGANIZE**  
a training specific  
for managers and personnel  
to detect pick up  
and  
report signs of concern

Measure Observation 38



Conduct  
**RANDOM CONTROLS**

Measure Observation 39



**4-EYES PRINCIPLE**

Measure Observation 40



**PREVENT**  
an employee  
from  
accessing data/facilities  
that (s)he doesn't need  
for the job  
*(role-based access)*

Measure Observation 41



Formally inform  
employees that  
activities  
during working hours  
**CAN BE CONTROLLED**  
by private investigators

Measure Observation 42



**ENCOURAGE**  
self-reporting

Measure Observation 43



Ensure the (higher)  
management is aware  
of the  
**INSIDER THREAT**

Measure Observation 44



Ensure an active role  
for the line manager  
when during a follow-up  
someone seemed  
**UNHAPPY**  
or different than usual

Measure Observation 45



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation



INSIDER THREAT  
MITIGATION



Universiteit  
Antwerpen

Measure Observation