Questionnaire Items:

Understanding information security compliance - Why goal setting and rewards for productivity might be a bad idea

Theory of planned behavior (Hu et. al, 2012)

Scale:
1 = strongly disagree [1]
2 = [2]
3 = [3]
4 = [4]
5 = strongly agree [5]
-1 = I cannot assess this question

Perceived Management Participation
PMP_01 Senior managers of our company have articulated a clear vision about information security.
PMP_02 Senior managers of our company have formulated a clear strategy for achieving a high degree of information security.
PMP_03 Senior managers of our company have established clear goals and objectives for achieving a high degree of information security.

Attitude
ATT_01 I believe that it is beneficial for an organization to establish clear information security policies, practices, and technologies.
ATT_02 I believe that it is useful to for an organization to enforce its information security policies, practices, and technologies.
ATT_03 I believe that it is a good idea for an organization to establish clear information security policies, practices, and technologies.

Subjective norm
SN_01 People who are influential to me would think that I should follow the policies and procedures and use the security technologies.
SN_02 People who are important to me would think that I should follow the policies and procedures and use the security technologies.
SN_03 People whom I respect would think that I should follow the policies and procedures and use the security technologies.

Perceived behavioral control
PBC_01 I am able to follow the policies and procedures and use the security technologies.
PBC_02 I have the resources and knowledge to follow the policies and procedures and use the security technologies.
PBC_03 I have adequate training and skills to follow the policies and procedures and use the security technologies.

Behavioral intention
INT_01 I intend to follow the information security policies and practices at work.
INT_02 I intend to use the information security technologies at work.
INT_03 I intend to use common sense on good information security practices at work.

Organizational culture (van Dyck, 2005)

Scale:
1 = strongly disagree [1]
2 = [2]
3 = [3]
4 = [4]
5 = strongly agree [5]
Error Management Culture
EMC_01 For us, errors are very useful for improving the work process.
EMC_02 After making a mistake, people try to analyze what caused it.
EMC_03 When an error is made, it is corrected right away.
EMC_04 Although we make mistakes, we don’t let go of the final goal.
EMC_05 An error provides important information for the continuation of the work.
EMC_06 If people are unable to continue their work after an error, they can rely on others.
EMC_07 When mastering a task, people can learn a lot from their mistakes.
EMC_09 After an error, people think through how to correct it.
EMC_10 When people are unable to correct an error by themselves, they turn to their colleagues.
EMC_11 When someone makes an error, (s)he shares it with others so that they don’t make the same mistake.
EMC_12 Our errors point us at what we can improve.
EMC_13 After an error has occurred, it is analyzed thoroughly.
EMC_14 When people make an error, they can ask others for advice on how to continue.
EMC_15 In this organization, people think a lot about how an error could have been avoided.
EMC_16 If something went wrong, people take the time to think it through.
EMC_17 When an error has occurred, we usually know how to rectify it.

Error Aversion Culture
EAC_01 There are advantages in covering up one’s errors.
EAC_02 Our motto is, “Why admit an error when no one will find out?”

Commitment towards the organization (Schmidt et al., 1998)

Scale:
1 = strongly disagree [1]
2 = [2]
3 = [3]
4 = [4]
5 = strongly agree [5]

AC_01 I do not have a strong sense of belonging for my coganization. (R)
AC_02 This organization has a great personal meaning for me.
AC_03 I would be very happy to spend my further working life in this organization.
AC_04 I enjoy talking about my organization even with persons that do not work here.
AC_05 Problems of my organization often bother me as if they were my own problems.

Information quality (Lee et al., 2002)

Scale:
1 = strongly disagree [1]
2 = [2]
3 = [3]
4 = [4]
5 = strongly agree [5]

Accessibility
ACCESS_01 This information is easily accessible.
ACCESS_02 This information is quickly accessible when needed.
ACCESS_03 This information is easily retrievable.

Appropriate Amount
APP_AM_01 This information is of sufficient volume for our needs.
APP_AM_02 The amount of information is not sufficient for our needs. (R)
APP_AM_03 The amount of information is neither too much nor too little.
Believability
BEL_01 This information is credible.

Completeness
COM_01 This information includes all necessary values.
COM_02 This information is incomplete. (R)
COM_03 This information is sufficiently complete for our needs.
COM_04 This information has sufficient breadth and depth for our task.

Concise Representation
CONC_REP_01 The representation of this information is compact and concise.

Consistent Representation
CONS_REP_01 This information is presented consistently.

Ease of Operation
EoO_01 This information is easy to aggregate.
EoO_02 This information is easy to combine with other information.

Free of Error
FoE_01 This information is correct.
FoE_02 This information is accurate.
FoE_03 This information is reliable.

Interpretability
INT_01 It is easy to interpret what this information means.

Relevancy
REL_01 This information is useful to our work.
REL_02 This information is relevant to our work.
REL_03 This information is appropriate for our work.
REL_04 This information is applicable to our work.

Security
SEC_01 This information can only be accessed by people who should see it.

Timeliness
TIME_01 This information is sufficiently current for our work.
TIME_02 This information is not sufficiently current for our work. (R)
TIME_03 This information is sufficiently up-to-date for our work.

Understandability
UND_01 The meaning of this information is difficult to understand. (R)

Actual compliance with security policies (self-constructed)

Scale:
1 = Never
2 = Rarely
3 = Occasionally
4 = Frequently
5 = Always

Have you ever avoided or tried to avoid following a security policy (for example: You need information from a certain file, but don’t have the right to access it. Since a request for access would take too long, you ask a colleague to send the file to you)?
Goal Setting (Putz & Lehner, 2002)

Scale:
1 = not at all
2 = rather not
3 = neutral
4 = rather yes
5 = totally

Participation
PAR_01 My supervisor informs me about the reasons why he assigns me specific goals.
PAR_02 My supervisor lets me participate in the formulation of my goals.

Dysfunctional Effects
DYS_01 Among me and my colleagues is a very computational atmosphere.
DYS_02 The pressure of achieving the goals leads to the whitewashing of facts.
DYS_03 The „upper ones“ in the organization do not give a good example for the employees, because they are not ingenuous by themselves.
DYS_04 If my supervisor makes a mistake that affects my possibilities to achieve my goals, he rejects to admit or discuss the mistake.
DYS_05 Most of my colleagues try to outperform one another concerning the given goals.
DYS_06 I don’t have much time to support my colleagues because I am usually busy myself. (self constructed)
DYS_07 Sometimes I take risks to achieve my given goals. (self constructed)
DYS_08 To achieve my goals, sometimes I have to depart from policies. (self constructed)
DYS_09 The quality of my work suffers from my demanding goal specifications. (self constructed)

Goal clarity
GCL_01 I have specific, clear goals to achieve in my area of operations.
GCL_02 I have unclear goals in my area of operations. (R)

Goal conflicts
GCO_01 Some goals given to me contradict with my personal ideals.
GCO_02 My goals limit themselves to merely short-term attainments and neglect long-term consequences.

Overstrain
OV_01 My goals are far too difficult.
OV_02 Often, it is not possible for me to achieve my goals.
OV_03 I have too many goals in my area of operations (I am overstrained).

Support
SUP_01 My supervisor supports me by encouraging me to pursue my goals.
SUP_02 In conversations with my supervisor about my performance, it is more important for him to solve problems than to criticize.
SUP_03 My supervisor lets me down if I have difficulties with a goal. (R)

Feedback
FE_01 I receive praise and appreciation if I achieve my goals.
FE_02 I receive feedback about my performance concerning my goals regularly.
FE_03 My supervisor informs me why I deserve appreciation in his opinion during meetings about my work and tasks.

Reward
REW_01 My chances to receive a salary increase raise if I achieve my goals.
REW_02 My chances to get promoted raise if I achieve my goals.
REW_03 To some extent, my salary depends on the achievement of my goals.

Resources
RES_01 The departments in our organization cooperate to achieve goals.
RES_02 The organization provides appropriate resources (time, money, equipment, employees) in order to work goal-oriented.
RES_03 I recieve beneficial on-the-job training to be able to achieve my goals..

Further investigation of employees’ security policy compliance (self-constructed)

FI_01 Did you get informed of or trained about information security at the beginning of your current employment?

FI02 Based on your experience, do employees always comply to security policies or do they sometimes except to the policies?

FI03 Do you feel constrained in your daily work due to the security policies?

FI_04 Do you have the impression that your current employer informs about security policies too little, too much or just right?

FI_05 Is compliance with security policies monitored (e.g., at workshops or by random examination of access authorization)?

FI_06 Do you feel generally taken serious at intra-company discussions about security policies?

FI_07 Are you granted enough time to talk about your problems and concerns related to information security?

FI08 Do you have the impression that the 'same language' is spoken in discussions about security policies?

FI09 If you could change anything in communication about information security, what would you want to change? What communication procedures would you want in the future?

Demografie (self-constructed)

Thank you very much for your participation!

Finally, we ask you to provide some information about your person. These information is exclusively used for analysis of our study and not handed on to third persons.

DE01 Gender
1 = Male
2 = Female
3 = Other

DE02 Age
1 = < 20
2 = 20-25
3 = 26-35
4 = 36-45
5 = 46-55
6 = 56-65
7 = 66-75
DE03 Highest educational attainment
1 = Certificate of Secondary Education
2 = General Certificate of Secondary Education
3 = A levels
4 = University degree
5 = Master craftman's diploma
6 = Doctor
7 = Habilitation
8 = Others, namely (open text input)

DE04 How much experience do you have concerning IT/computer?
1 = very little [1]
2 = [2]
3 = [3]
4 = [4]
5 = very much [5]

DE05 How many employees does your current employer/organization hold?
1 = < 10
2 = 11-24
3 = 25-49
4 = 50-99
5 = 100-499
6 = 500-999
7 = 1.000-4.999
8 = 5.000-99.999
9 = > 100.000

DE06 In which domain is your organization located?
1 = Education
2 = Services, Consulting
3 = Retail, Wholesale
4 = Production
5 = Finances
6 = Research
7 = Health
8 = Real estate
9 = Industry
10 = Information technology
11 = Grocery, Household goods
12 = Medicine, Bio technology, Pharmacy
13 = Nonprofit
14 = Government
15 = Travel
16 = Telecommunication
17 = Others, namely (open text input)

DE07 How many percent of your total salary is variable (e.g., depends on bonuses for goal achievement)?
1 = 0%
101 = 100%
-1 = I don’t know/does not apply
DE08.1 What is your current job amount?

1 = full time

2 = part time (please provide number of hours per week): (open text input)